Collection EXPERT IT

Windows Server 2008

Administration avancée

Mathieu CHATEAU

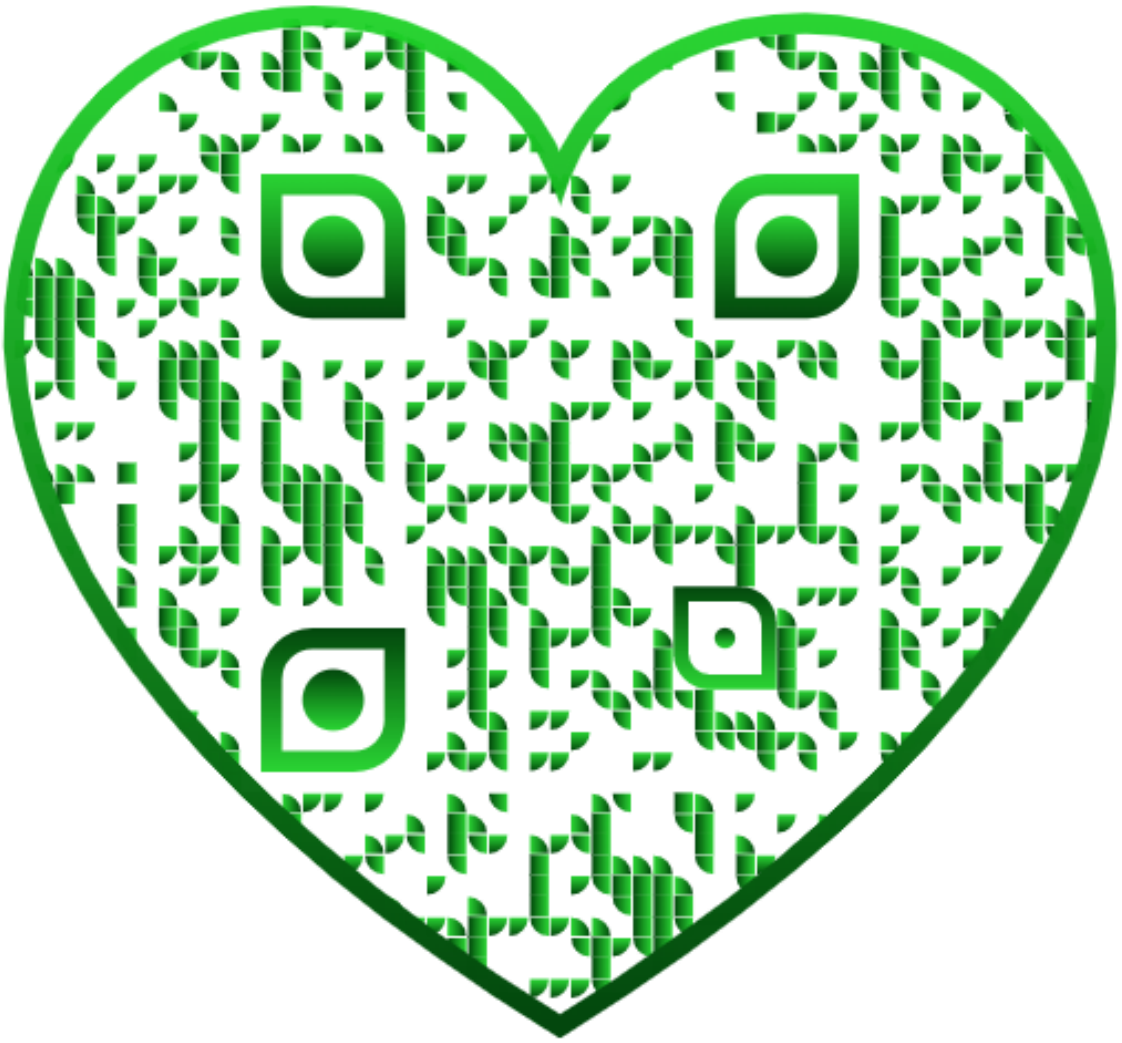
Thierry DEMAN

Freddy ELMALEH

Sébastien NEILD

Microsoft GOLD CERTIFIED Partner

eni Editions



Windows Server 2008

Administration avancée

Thierry DEMAN - Freddy ELMALEH - Mathieu CHATEAU - Sébastien NEILD

Résumé

Ce livre s'adresse aux **administrateurs et ingénieurs systèmes** désireux d'acquérir et de maîtriser des connaissances approfondies sur Windows Server 2008.
Il répond aux besoins d'expertise du lecteur en traitant de façon approfondie, d'un point de vue théorique et pratique, des rôles incontournables comme **Active Directory, DFS, Hyper-V** ou encore le **VPN**.
Les **nouveautés R2** de Windows Server 2008 sont également expliquées afin d'anticiper au mieux l'avenir.
Depuis le **déploiement** jusqu'à la **virtualisation**, cet ouvrage est le compagnon idéal pour appréhender les moindres détails de cette version de Windows Server. Il apporte un haut niveau d'expertise et son ambition est de devenir un livre de référence.
Les auteurs mettent au service du lecteur **leur expertise Microsoft** (MVP, MCSE et/ou MCITP) et leur expérience très significative dans des **infrastructures conséquentes et complexes**, afin de fournir un livre de qualité respectant les meilleures pratiques du monde de l'entreprise.

L'auteur

Thierry Deman est Architecte systèmes et maîtrise les technologies Microsoft depuis de nombreuses années au sein du Permis Informatique. Il est reconnu Microsoft MVP (Most Valuable Professional) sur Exchange depuis plusieurs années et est certifié MCITP Exchange 2007 et MCITP Enterprise Administrator sur Windows Server 2008.

Freddy Elmaleh est consultant freelance, architecte systèmes et chef de projet, expert Active Directory et Sécurité, fondateur de la société de services Active IT. Il intervient au sein de nombreuses grandes entreprises. Il est reconnu Microsoft MVP (Most Valuable Professional) sur Windows Server - Directory Services depuis plusieurs années et est certifié MCSE Securité/Messagerie et MCITP Enterprise Administrator sur Windows Server 2008.

Mathieu Chateau est Architecte Technique dans un grand groupe financier et à ce titre intervient tant dans la définition des architectures que dans la gestion de la sécurité, du réseau et dans l'administration des solutions de haute disponibilité.

Sébastien Neild est Ingénieur Systèmes et Réseaux dans une société de service. Il intervient en tant que responsable de projets Active Directory et Exchange et a participé à de nombreux projets de déploiement et migration d'infrastructures Windows Server. Il est certifié MCSE et MCITP Server Administrator sur Windows Server 2008.

Ce livre numérique a été conçu et est diffusé dans le respect des droits d'auteur. Toutes les marques citées ont été déposées par leur éditeur respectif. La loi du 11 Mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective", et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause, est illicite" (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal. Copyright Editions ENI

Introduction

Ce livre traite du dernier système d'exploitation de la gamme Windows Server de Microsoft.

Il s'agit bien entendu de Windows Server 2008.

Windows Server 2008 a été pensé par Microsoft pour offrir une plate-forme souple et complète afin de répondre aux besoins sans cesse grandissant des entreprises. Vous pouvez ainsi profiter de nouvelles fonctionnalités à la fois utiles et judicieuses vous permettant de faire reposer l'ensemble de votre système d'information sur une solution Microsoft.

© ENI Editions - All rigths reserved

Les différentes éditions de Windows Server 2008

Comme à l'accoutumée, Microsoft Windows Server 2008 est disponible sous différentes éditions. Il n'existe pas moins de 9 versions différentes de ce système d'exploitation.

- Windows Server 2008 Edition Standard (x86 et x64) avec ou sans Hyper-V
- Windows Server 2008 Edition Enterprise (x86 et x64) avec ou sans Hyper-V
- Windows Server 2008 Edition Datacenter (x86 et x64) avec ou sans Hyper-V
- Windows HPC Server 2008
- Windows Web Server 2008 (x86 et x64)
- Windows Storage Server 2008 (x86 et x64)
- Windows Small Business Server 2008 (x64) pour les PE
- Windows Essential Business Server 2008 (x64) pour les PME
- Windows Server 2008 pour Systèmes Itanium-based

Elles sont toutes disponibles en version X86 (32 bits et 64 bits) sauf la version Itanium.

La version Itanium est compatible avec les processeurs IA64 dont l'architecture est optimisée pour le traitement des bases de données et des applications *Line of Business* (LOB).

À noter également que la version R2 de Windows Server 2008 ne peut être installée que sur une version 64 bits.

Vous trouverez un descriptif détaillé de ces différentes versions sur le site suivant : http://www.microsoft.com/windowsserver2008/en/us/editions.aspx (en anglais)

© ENI Editions - All rigths reserved

Les grands axes de Windows Server 2008

Lors de l'étude des axes majeurs à suivre pour cette version de Windows Server, Microsoft a pris en considération la charge de travail et la pression sur le service IT des entreprises qui est sans cesse grandissante. Il fallait donc que ce système d'exploitation réponde à trois exigences essentielles.

1. Un meilleur contrôle de l'information

Windows Server 2008 propose un meilleur contrôle de l'information afin de garantir une meilleure efficacité d'administration et par conséquent une meilleure productivité.

Afin d'augmenter cette qualité d'administration, Windows Server 2008 possède la capacité de scripts et d'automatisation de tâches accrues grâce à son nouveau langage de script Microsoft **Windows Powershell**. L'automatisation des tâches courantes d'administration se voit ainsi grandement améliorée et flexible grâce à cette nouvelle fonctionnalité.

L'installation basée sur les rôles et fonctionnalités grâce à la console unique **Gestionnaire de serveur** facilite l'administration. Les assistants disponibles permettent de limiter au maximum les erreurs de configuration grâce aux nombreuses explications qui viennent accompagner l'administration lors de l'installation d'un composant Windows.

Microsoft propose également la possibilité d'installer une version minimale de Windows Server 2008, connue aussi sous le nom de **Windows Server Core**. Windows Server 2008 fonctionne alors sans interface graphique et tout doit donc être configuré en ligne de commande. L'avantage majeur de ce type d'installation réside dans le fait que la surface d'attaque est réduite de par le fait que le strict minimum est installé sur le serveur. Les administrateurs viendront alors ajouter les rôles de leurs choix. Afin de ne pas trop exposer ces serveurs, le .NET Framework n'est pas installé et l'exécution de code comme PowerShell n'est donc pas possible.

Des nouvelles consoles comme le **moniteur de performance et de fiabilité** permettent également de détecter en amont des problèmes de configuration sur vos systèmes d'exploitation et d'en informer automatiquement le service informatique. Il offre également beaucoup d'informations précises sur l'utilisation des composants système de votre choix.

Enfin, dernière bonne nouvelle pour les administrateurs, une meilleure gestion de l'impression est désormais possible ! En effet, les imprimantes peuvent être automatiquement installées sur les ordinateurs des utilisateurs à l'aide de stratégies de groupe.

Une nouvelle console MMC vous permet de mieux gérer, contrôler et dépanner les imprimantes de votre domaine.

2. Une meilleure protection du système d'information

Microsoft a totalement retravaillé le noyau de Windows Server 2008 comparé au noyau de ses prédécesseurs. Celui-ci présente de nombreuses similitudes avec celui de Windows Vista puisque les deux systèmes d'exploitation se basent sur le nouveau noyau répondant au nom de NT6 (Windows 2000 et XP reposaient sur le noyau NT 5.x).

Ce noyau possède ainsi la nouvelle technologie **Patchguard** développée par Microsoft afin de protéger au maximum le système d'exploitation et ainsi mettre un terme au rootkit ou autre attaque visant à modifier le noyau système.

La **protection de l'accès réseau (NAP)** devient également accessible et vous permet de mettre en place des conditions d'utilisations de votre réseau d'entreprise. Exit donc les personnes externes arrivant avec un ordinateur portable qui n'est pas à la norme de l'entreprise ou bien l'utilisateur n'ayant pas un antivirus à jour ! L'accès au réseau leur est refusé tant qu'ils ne remplissent pas les critères de conformité que vous aurez jugés nécessaires.

Les **contrôleurs de domaine en lecture seule (RODC)** renforcent la sécurité de vos domaines Active Directory dans la mesure où vous pouvez limiter la diffusion de certains mots de passe en cas de compromission de ces contrôleurs de domaine. Ces derniers trouveront par exemple leur place dans des petits réseaux d'agence où la sécurité physique du contrôleur de domaine ne pourra être garantie.

Les nouveaux services associés à l'Active Directory renforcent également la sécurité de votre informatique. Le rôle **AD CS** *(Active Directory Certificate Services)* permet la diffusion de certificats basés sur la cryptographie nouvelle génération (CNG). Le rôle **AD RMS** *(Active Directory Rights Management Services)* vous donne la possibilité de maîtriser la diffusion des documents de votre entreprise.

Le **pare-feu avancé** de Windows Server 2008 permet de limiter la surface d'attaque de votre serveur en faisant un filtrage de ports sur le trafic réseau entrant ou sortant. Le pare-feu analyse le flux au niveau applicatif et vous pourrez donc n'autoriser un trafic que pour un service spécifique. De plus, la nouvelle console de gestion MMC pour le pare-feu avancé permet de configurer des flux **IPSec** afin d'assurer l'intégrité ou chiffrer le flux entre ordinateurs. Cela est idéal pour définir un chiffrement entre des contrôleurs de domaine ou entre des postes d'administrateurs de domaine et des serveurs d'administration.

Le chiffrement de lecteur disque avec l'outil **Bitlocker** permet également d'empêcher l'accès aux données de votre

© ENI Editions - All rigths reserved

disque dur depuis une installation parallèle d'un autre système d'exploitation.

Les fonctionnalités de sécurité présentes sous Windows Server 2008 permettent donc de limiter au maximum le risque d'attaque sur le serveur tout en garantissant une productivité et une flexibilité importante.

3. Une plate-forme évolutive

Windows Server 2008 est une plate-forme capable de s'adapter et de répondre ainsi au besoin d'évolution d'une société.

La technologie **hyperviseur (Hyper-V)** 64 bits répond au besoin grandissant des entreprises souhaitant virtualiser certains de leurs serveurs. Cette technologie répond ainsi de façon ultra-réactive aux charges de travail dynamiques.

Les services **Terminal Server** apportent un lot d'innovations qui va beaucoup améliorer l'expérience utilisateur.

Un accès centralisé aux applications peut en effet être défini afin de décorréler petit à petit le poste de travail des applications qui sont nécessaires aux utilisateurs.

Il vous est ainsi possible de rendre disponibles des applications (publication d'applications) sans que celles-ci soient installées sur l'ordinateur de l'utilisateur. Le raccourci de l'application apparaît alors sur le bureau de l'utilisateur au côté des applications installées localement sur son ordinateur. L'utilisateur ne peut donc pas, à première vue, distinguer les applications locales de celles déportées, ce qui vous fait également gagner du temps en terme de formation des utilisateurs.

Un service de **passerelle Terminal Services** (appelé aussi TS Gateway) ne vous oblige plus à multiplier les ports à ouvrir sur votre réseau ou à monter un réseau privé virtuel. Un unique point d'entrée, via un portail web, vous permet d'accéder à votre réseau d'entreprise. Le trafic RDP est en effet encapsulé de façon transparente dans un flux SSL (HTTPS).

L'**accès web aux services Terminal Server** (TS Web Access) est une interface web permettant l'accès aux applications RemoteApp que vous avez choisi de publier. Ces applications sont ainsi accessibles depuis votre navigateur internet. Cette solution s'appuie sur IIS et peut également être intégrée à un portail Sharepoint.

Grâce à Windows Server 2008, vous pouvez gérer les évolutions de la société et en particulier les applications ayant des besoins de haute disponibilité.

Le **cluster de serveurs** a pour principe de contenir plusieurs serveurs ayant un rôle identique. Si un des serveurs (appelés nœud du cluster) devient indisponible, le système de cluster vous bascule automatiquement vers un autre nœud disponible. Cela se fait sans aucune intervention des administrateurs, ce qui limite alors la durée d'indisponibilité d'une application.

Le service de haute disponibilité se caractérise également par la possibilité de faire de l'**équilibrage de la charge réseau** (appelé également NLB pour *Network Load Balancing*). Cet équilibrage permet de répartir la charge réseau entre plusieurs serveurs présentant les mêmes informations. L'équilibrage de charge réseau peut ainsi répondre à un fort développement de l'activité d'un site Internet par exemple en choisissant de diriger les demandes de connexion au serveur web vers le serveur IIS le moins occupé.

Enfin le cycle de vie de votre serveur devient plus simple à gérer avec un ensemble d'outils adaptés et performants.

Parmi ceux-ci nous pouvons citer la fonctionnalité de **sauvegarde** qui permet de gérer vos sauvegardes et restaurations à partir d'assistants très intuitifs. La technologie de clichés instantanés permet de sauvegarder vos fichiers en cours d'exécution de façon quasi immédiate.

Le serveur de patchs **WSUS3** permet de gérer l'ensemble des mises à jour (correctifs, patchs de sécurité) des systèmes d'exploitation et certaines applications Microsoft au sein de votre réseau d'entreprise.

Ce livre a ainsi pour but de vous présenter les principales fonctionnalités de Windows Server 2008.

Il sera parsemé d'avis et de conseils d'experts Microsoft et s'adresse ainsi à des personnes ayant déjà acquis une certaine expérience. Néanmoins, cet ouvrage s'est également attaché à expliquer les concepts de base afin d'être ainsi facilement accessible aux personnes n'ayant pas d'expérience notoire avec la technologie serveurs de Microsoft.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre est consacré à l'annuaire Microsoft Active Directory. Le service d'annuaire Microsoft est devenu indispensable dans la gestion de l'information au sein d'une entreprise.

Dans une première partie, une présentation du service d'annuaire sous Windows Server 2008 sera abordée. Suivront alors des explications sur les principaux composants attachés au service d'annuaire comme les stratégies de groupes et des autres services attachés au service d'annuaire Microsoft.

© ENI Editions - All rigths reserved

Présentation du service d'annuaire Microsoft : Active Directory Domain Services

Vous connaissez sans doute le principe de fonctionnement de l'annuaire Active Directory. Cet ouvrage n'ayant pas pour but de réexpliquer ce que vous savez déjà, les grands principes d'un annuaire Active Directory (appelé désormais Active Directory Domain Services ou AD DS) seront traités de façon succincte pour ainsi pouvoir concentrer votre attention sur les spécificités apportées par Windows Server 2008.

1. Définition d'un domaine Active Directory

Active Directory est un service d'annuaire permettant de référencer et d'organiser des objets comme des comptes utilisateurs, des noms de partages, des autorisations à l'aide de groupes de domaine, etc. Les informations peuvent ainsi être centralisées dans un annuaire de référence afin de faciliter l'administration du système d'information.

D'un point de vue logique, trois notions sont à retenir :

- Le domaine est l'unité de base chargée de regrouper les objets qui partagent un même espace de nom (un domaine doit en effet nécessairement se reposer sur un système DNS, supportant les mises à jour dynamiques et les enregistrements de type SRV).

- Une arborescence de domaines est le regroupement hiérarchique de plusieurs domaines partageant un même espace de nom (par exemple les domaines lyon.masociete.local et paris.masociete.local).

- Une forêt consiste à regrouper plusieurs arborescences de domaine qui ont en commun un catalogue global et qui ne partagent pas forcément un espace de nom commun.

D'un point de vue physique, trois principaux éléments sont à retenir :

- Les contrôleurs de domaine sont chargés de stocker l'ensemble des données et de gérer les interactions entre les utilisateurs et le domaine (ouverture de session, recherche dans l'annuaire, etc.). Contrairement aux anciens systèmes NT, une réplication multimaître a lieu sur un domaine, ce qui permet ainsi à n'importe quel contrôleur de domaine de pouvoir initier une modification (ajout d'un compte utilisateur, changement d'un mot de passe utilisateur, etc.).

- Chaque contrôleur de domaine contient également des partitions. Microsoft a décidé de partager l'information en plusieurs partitions afin de pouvoir limiter l'étendue des données à répliquer. Chaque partition n'a donc pas la même étendue de réplication. Tous les contrôleurs de domaine d'une même forêt ont les partitions de **schéma** et de **configuration** en commun. Une modification sur une de ces partitions n'engendrera donc une réplication que vers certains contrôleurs de domaine.

  Tous les contrôleurs de domaine d'un même domaine partagent une partition de **domaine** commune.

  La quatrième partition (présente de façon facultative) est la partition d'**application**. Celle-ci stocke les données sur les applications utilisées dans Active Directory et se réplique sur les contrôleurs de domaine de votre choix faisant partie de la même forêt.

- Les sites Active Directory mettent en évidence le regroupement physique d'objets sur un domaine. Vous devez en outre attacher un (ou des) contrôleur(s) de domaine à un même site Active Directory si ces contrôleurs de domaine communiquent avec un lien réseau ayant un bon débit. En effet, les contrôleurs de domaine d'un même site dialoguent de façon beaucoup plus fréquente que des contrôleurs de domaine définis sur deux sites Active Directory distincts. Cela vous permettra ainsi de réduire de façon non négligeable le trafic réseau sur un lien distant séparant vos deux sites.

2. Fonctionnalités de l'Active Directory sous Windows Server 2008

Windows Server 2008 propose un grand nombre de fonctionnalités. Celles-ci raviront aussi bien les personnes n'ayant pas de connaissances préalables que celles désireuses d'en savoir davantage.

Il vous sera ainsi expliqué comment installer un contrôleur de domaine Active Directory avec Windows Server 2008, comment utiliser les stratégies de mot de passe affinées, etc.

Ces fonctionnalités vous seront présentées par des travaux pratiques et concrets afin que vous puissiez constater de

© ENI Editions - All rigths reserved

vous-même de l'utilité de ces dernières au travers de ce chapitre.

a. Installation d'un annuaire Active Directory

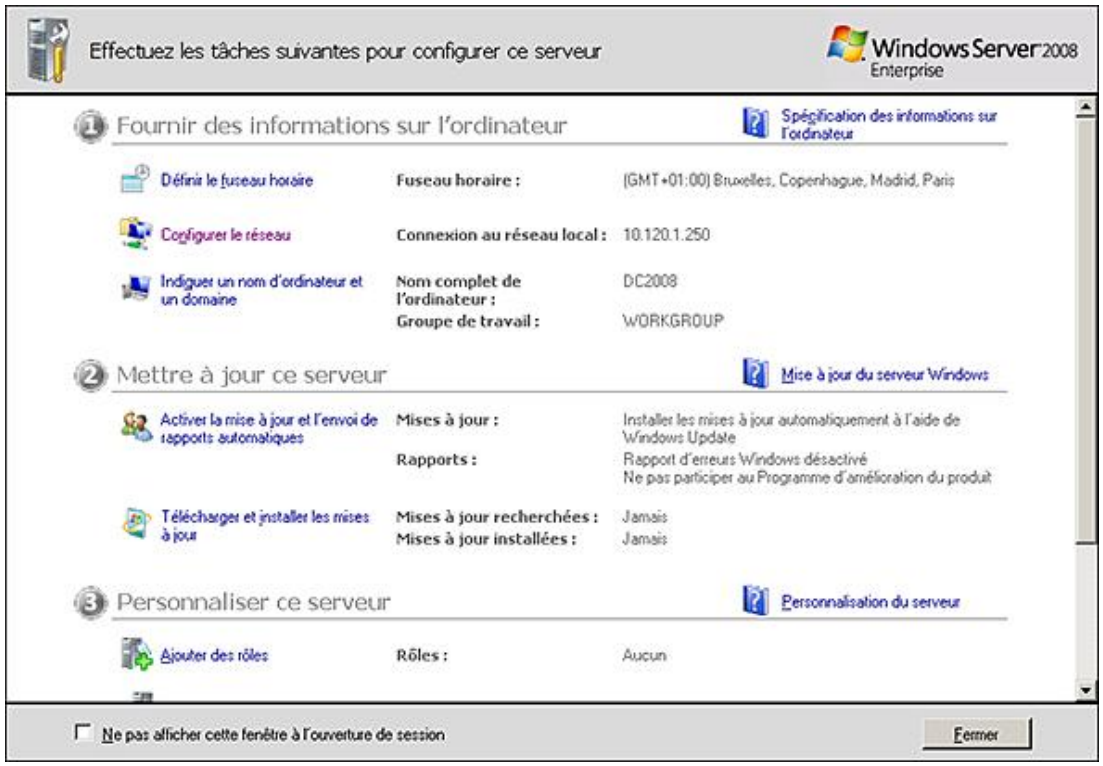
D'une façon générale, les assistants de configuration se sont beaucoup améliorés au fil des versions de Windows. Vous découvrirez rapidement que ces derniers sont très utiles et intuitifs. Par exemple, il vous est désormais possible de faire appel à la plupart des options avancées d'installation de l'annuaire Active Directory à partir de l'assistant créé à cet effet.

Windows 2008 arrive avec deux nouvelles notions. Celles de Rôles et de Fonctionnalités. Elles sont configurables à partir de la console **Gestionnaire de serveur**. Vous utiliserez donc cette console afin d'ajouter le rôle **Service de domaine Active Directory** (connu aussi sous le nom AD DS pour *Active Directory Domain Services*).

L'ensemble de ces manipulations doit être effectué avec un compte utilisateur possédant les droits Administrateur sur le serveur.

- Assurez-vous dans un premier temps que vous avez correctement défini le nom NETBIOS de votre futur contrôleur de domaine, ainsi qu'une adresse IP fixe valide. Il est toujours conseillé de définir ces paramètres avant la promotion d'un serveur en tant que contrôleur de domaine.

Par défaut, l'assistant **Tâches de configuration initiales** se lance à chaque démarrage de Windows afin de vous permettre de configurer votre serveur une fois installé.


Effectuez les tâches suivantes pour configurer ce serveur
Windows Server 2008 Enterprise
Fournir des informations sur l'ordinateur
Spécification des informations sur l'ordinateur
Définir le fuseau horaire
Fuseau horaire :
(GMT+01:00) Bruxelles, Copenhague, Madrid, Paris
Configurer le réseau
Connexion au réseau local :
10.120.1.250
Indiquer un nom d'ordinateur et un domaine
Nom complet de l'ordinateur :
DC2008
Groupe de travail :
WORKGROUP
Mettre à jour ce serveur
Mise à jour du serveur Windows
Activer la mise à jour et l'envoi de rapports automatiques
Mises à jour :
Installer les mises à jour automatiquement à l'aide de Windows Update
Rapports :
Rapport d'erreurs Windows désactivé
Ne pas participer au Programme d'amélioration du produit
Télécharger et installer les mises à jour
Mises à jour recherchées :
Jamais
Mises à jour installées :
Jamais
Personnaliser ce serveur
Personnalisation du serveur
Ajouter des rôles
Rôles :
Aucun
Ne pas afficher cette fenêtre à l'ouverture de session
Fermer

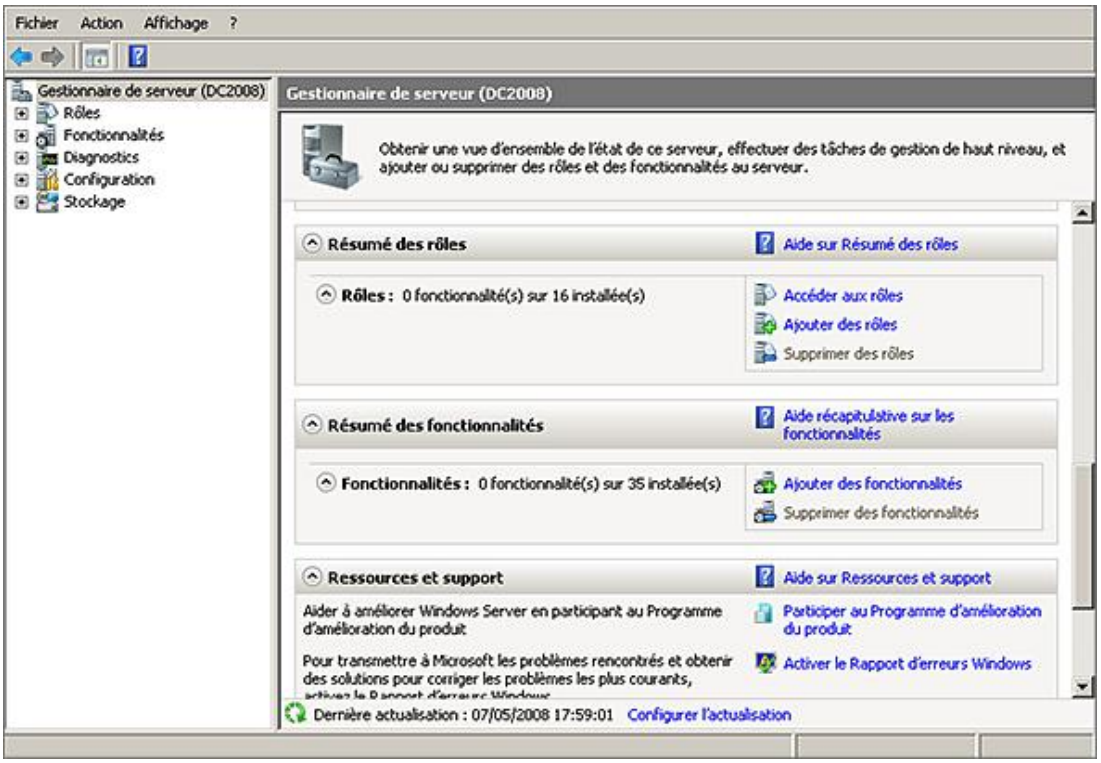
- Choisissez donc de configurer les options **Configurer le réseau** et **Indiquer un nom d'ordinateur et un domaine**. Vous pourrez ainsi définir une adresse IPv4 fixe, ainsi qu'un nom d'ordinateur évocateur pour votre serveur.

  Dans notre exemple, le nom d'ordinateur sera **DC2008** (DC pour *Domain Controller* ou Contrôleur de Domaine). Votre serveur devra alors être redémarré.

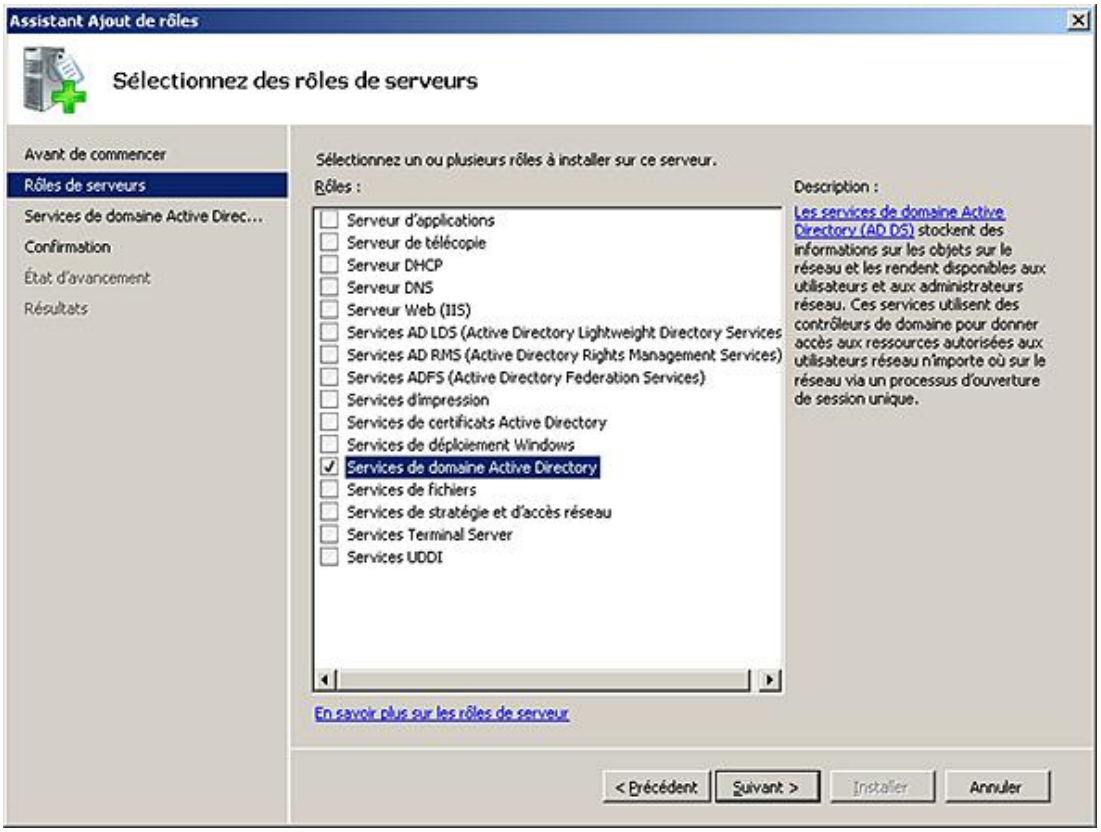
- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.

- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.

© ENI Editions - All rigths reserved


Fichier Action Affichage ?
Gestionnaire de serveur (DC2008)
Rôles
Fonctionnalités
Diagnostics
Configuration
Stockage
Gestionnaire de serveur (DC2008)
Obtenir une vue d'ensemble de l'état de ce serveur, effectuer des tâches de gestion de haut niveau, et ajouter ou supprimer des rôles et des fonctionnalités au serveur.
Résumé des rôles
Aide sur Résumé des rôles
Rôles : 0 fonctionnalité(s) sur 16 installée(s)
Accéder aux rôles
Ajouter des rôles
Supprimer des rôles
Résumé des fonctionnalités
Aide récapitulative sur les fonctionnalités
Fonctionnalités : 0 fonctionnalité(s) sur 35 installée(s)
Ajouter des fonctionnalités
Supprimer des fonctionnalités
Ressources et support
Aide sur Ressources et support
Aider à améliorer Windows Server en participant au Programme d'amélioration du produit
Participer au Programme d'amélioration du produit
Pour transmettre à Microsoft les problèmes rencontrés et obtenir des solutions pour corriger les problèmes les plus courants,
Activer le Rapport d'erreurs Windows
Dernière actualisation : 07/05/2008 17:59:01
Configurer l'actualisation

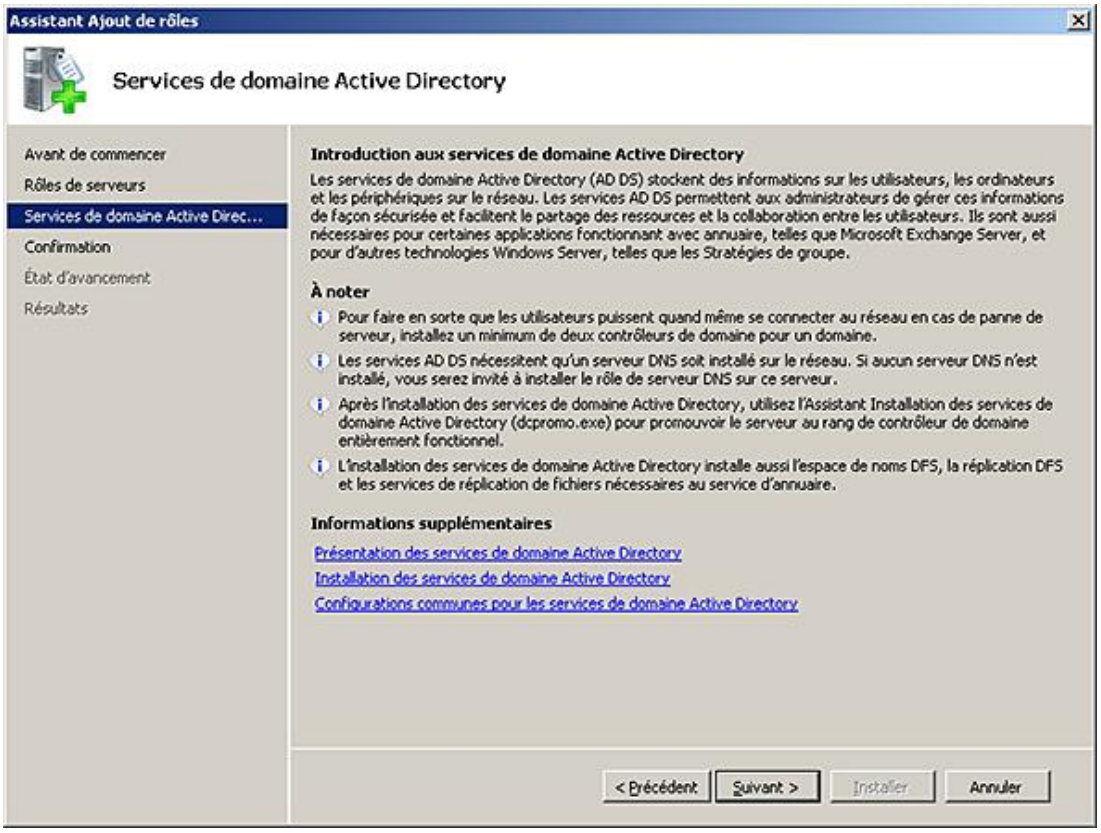
- L'**Assistant Ajout de rôles** s'ouvre alors. La première page est une page présente par défaut à chaque lancement de l'assistant. Celle-ci a pour but de vous faire vérifier un ensemble de bonnes pratiques avant de continuer à installer un rôle sur votre serveur (mot de passe fort, IP statique, correctifs de sécurité à jour). Cliquez sur **Suivant**. Choisissez alors de cocher le rôle que vous souhaitez installer. Comme vous souhaitez installer un contrôleur de domaine Active Directory, il vous faut choisir **Services de domaine Active Directory**. Les étapes suivantes de l'assistant se mettent à jour de façon dynamique en fonction du rôle choisi. Cliquez alors sur **Suivant**.


Assistant Ajout de rôles
Sélectionnez des rôles de serveurs
Avant de commencer
Rôles de serveurs
Services de domaine Active Direc...
Confirmation
État d'avancement
Résultats
Sélectionnez un ou plusieurs rôles à installer sur ce serveur.
Rôles :
Serveur d'applications
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Services AD LDS (Active Directory Lightweight Directory Services)
Services AD RMS (Active Directory Rights Management Services)
Services ADFS (Active Directory Federation Services)
Services d'impression
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory
Services de fichiers
Services de stratégie et d'accès réseau
Services Terminal Server
Services UDDI
Description :
Les services de domaine Active Directory (AD DS) stockent des informations sur les objets sur le réseau et les rendent disponibles aux utilisateurs et aux administrateurs réseau. Ces services utilisent des contrôleurs de domaine pour donner accès aux ressources autorisées aux utilisateurs réseau n'importe où sur le réseau via un processus d'ouverture de session unique.
En savoir plus sur les rôles de serveur
< Précédent
Suivant >
Installer
Annuler

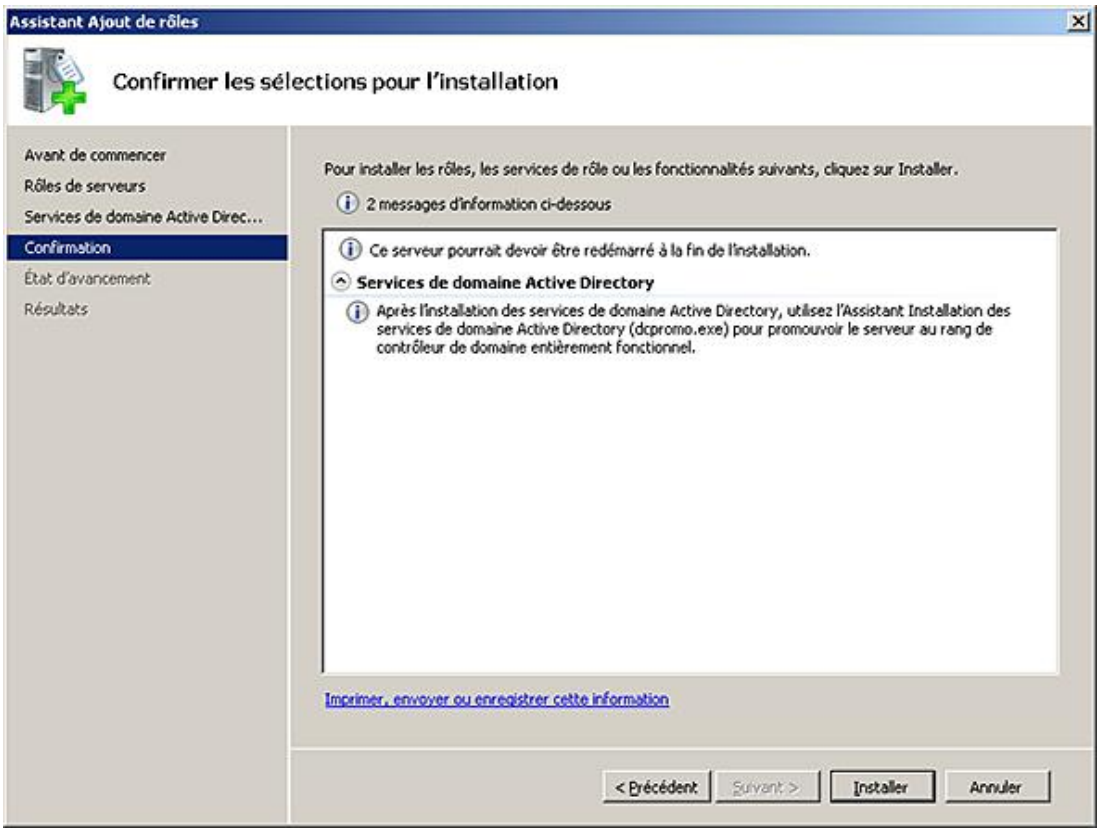
- L'assistant vous explique rapidement le rôle des services de domaine Active Directory et les principales informations à retenir. Il vous invite également à consulter des articles disponibles dans l'aide Windows pour plus

© ENI Editions - All rigths reserved

de renseignements. Cliquez sur **Suivant**.

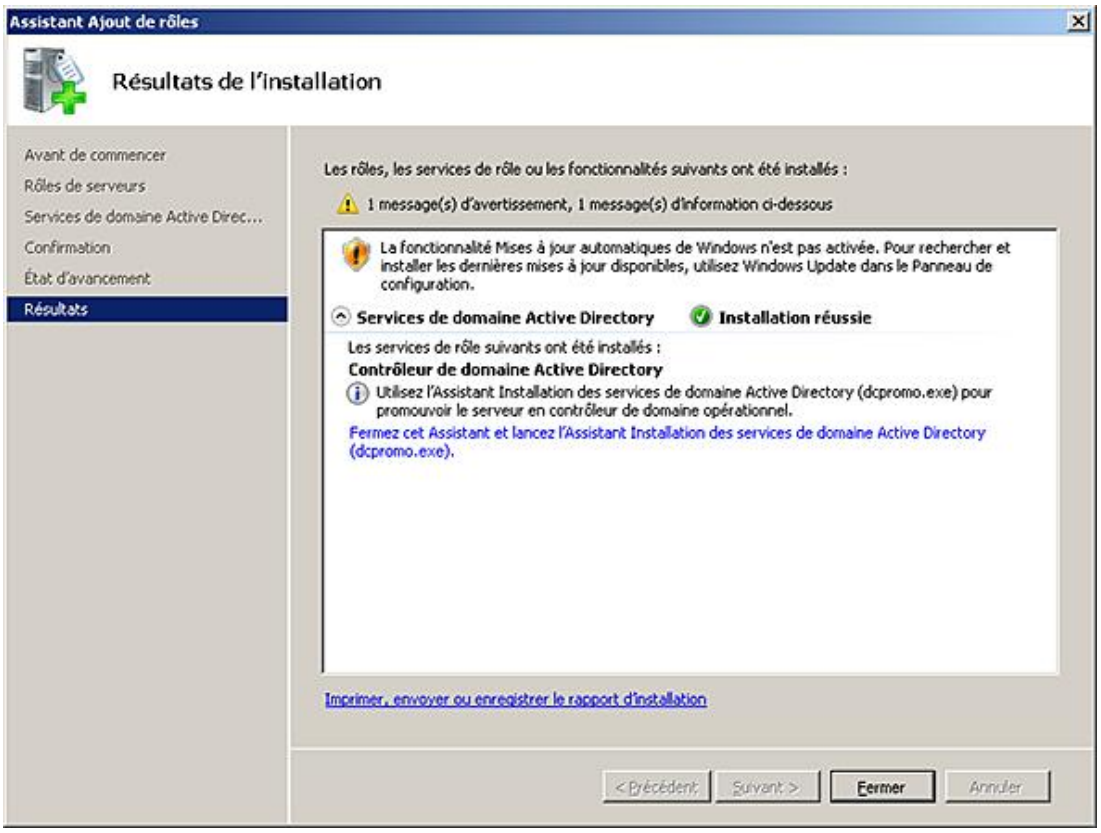

Assistant Ajout de rôles
Services de domaine Active Directory
Avant de commencer
Rôles de serveurs
Services de domaine Active Direc...
Confirmation
État d'avancement
Résultats
Introduction aux services de domaine Active Directory
Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs. Ils sont aussi nécessaires pour certaines applications fonctionnant avec annuaire, telles que Microsoft Exchange Server, et pour d'autres technologies Windows Server, telles que les Stratégies de groupe.
À noter
Pour faire en sorte que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine pour un domaine.
Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur ce serveur.
Après l'installation des services de domaine Active Directory, utilisez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour promouvoir le serveur au rang de contrôleur de domaine entièrement fonctionnel.
L'installation des services de domaine Active Directory installe aussi l'espace de noms DFS, la réplication DFS et les services de réplication de fichiers nécessaires au service d'annuaire.
Informations supplémentaires
Présentation des services de domaine Active Directory
Installation des services de domaine Active Directory
Configurations communes pour les services de domaine Active Directory
< Précédent
Suivant >
Installer
Annuler

- La dernière étape consiste à confirmer l'installation du rôle en question. Les messages d'information vous mettent en garde car le serveur devra être redémarré à la fin de l'installation. Une étape supplémentaire consistera à exécuter la commande **dcpromo** pour compléter l'installation du contrôleur de domaine. Cliquez sur **Installer**. L'installation du rôle débute alors.


Assistant Ajout de rôles
Confirmer les sélections pour l'installation
Avant de commencer
Rôles de serveurs
Services de domaine Active Direc...
Confirmation
État d'avancement
Résultats
Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer.
2 messages d'information ci-dessous
Ce serveur pourrait devoir être redémarré à la fin de l'installation.
Services de domaine Active Directory
Après l'installation des services de domaine Active Directory, utilisez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour promouvoir le serveur au rang de contrôleur de domaine entièrement fonctionnel.
Imprimer, envoyer ou enregistrer cette information
< Précédent
Suivant >
Installer
Annuler

© ENI Editions - All rigths reserved

- Une fois l'installation terminée, vous vous rendrez rapidement compte de la puissance et de l'utilité des assistants de Windows Server 2008. Ces derniers vérifient sans cesse si votre serveur répond aux critères de bases en termes de sécurité et de configuration. Dans cet exemple, l'assistant alerte sur le fait que la fonctionnalité **Mises à jour automatiques de Windows** n'est pas activée (si vous ne l'aviez pas déjà activée bien entendu). Il vous indique également la suite à effectuer afin de mener à bien cette installation. Cliquez sur le lien **Fermez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe)**. Vous pourrez également choisir de lancer cette commande un peu plus tard en l'exécutant directement depuis le menu **Démarrer - Exécuter - Dcpromo.exe**.


Assistant Ajout de rôles
Résultats de l'installation
Avant de commencer
Rôles de serveurs
Services de domaine Active Direc...
Confirmation
État d'avancement
Résultats
Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés :
1 message(s) d'avertissement, 1 message(s) d'information ci-dessous
La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour rechercher et installer les dernières mises à jour disponibles, utilisez Windows Update dans le Panneau de configuration.
Services de domaine Active Directory
Installation réussie
Les services de rôle suivants ont été installés :
Contrôleur de domaine Active Directory
Utilisez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) pour promouvoir le serveur en contrôleur de domaine opérationnel.
Fermez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe).
Imprimer, envoyer ou enregistrer le rapport d'installation
< Précédent
Suivant >
Fermer
Annuler

Si le contrôleur de domaine que vous prévoyez d'installer rejoint une forêt et/ou un domaine existant ayant un niveau fonctionnel de schéma ou de domaine Windows 2000 ou 2003, il vous faudra impérativement mettre à jour le niveau fonctionnel de la forêt et du (ou des) domaine(s) impacté(s). Pour cela, insérez le DVD de Windows Server 2008 dans votre contrôleur de domaine hébergeant le rôle de maître de schéma. Rendez-vous alors dans le dossier **sources\adprep** du DVD et lancez la commande `adprep /forestprep` (avec un compte utilisateur membre des groupes d'administrateurs de l'entreprise, du schéma et du domaine). Une fois cette opération terminée, laissez le temps à la réplication d'opérer puis mettez à jour le niveau fonctionnel du domaine sur lequel sera installé votre nouveau contrôleur de domaine. Pour ce faire, insérez le DVD de Windows Server 2008 dans un contrôleur de domaine du domaine impacté. Choisissez de préférence le contrôleur de domaine ayant le rôle de Maître d'infrastructure. Lancez alors la commande suivante `adprep /domainprep /gpprep`.

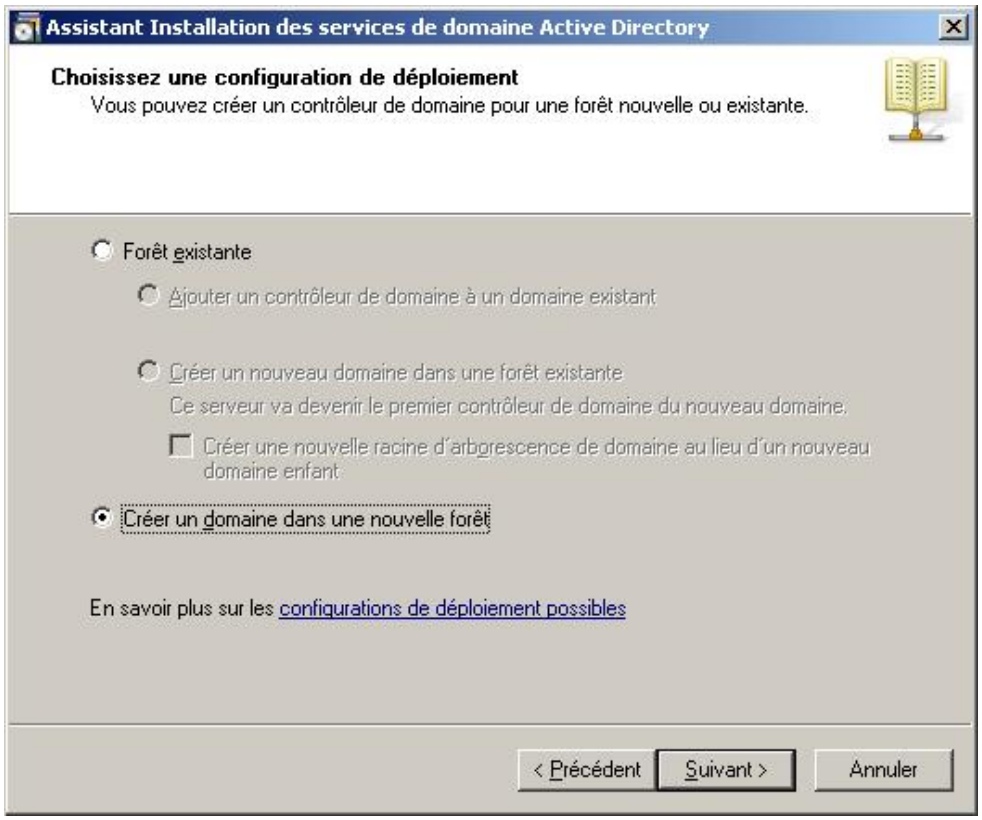
- L'**Assistant Installation des services de domaine Active Directory** se lance alors. Choisissez d'**Utiliser l'installation en mode avancé**. Cliquez sur **Suivant**.

  Un message d'avertissement indique les problèmes que vous risquez de rencontrer du fait de l'amélioration de l'algorithme de chiffrement utilisé à l'établissement d'un canal de sécurité avec un client SMB. Par défaut, les anciens systèmes d'exploitation comme Windows NT 4.0 ne pourront pas, par exemple, accéder à des partages se trouvant sur un serveur Windows 2008.

- Cliquez sur **Suivant** (si aucun serveur DNS n'est défini dans les propriétés de votre serveur, un message vous demandera de configurer un serveur DNS ou d'installer automatiquement le service DNS sur le serveur).

- Choisissez une configuration de déploiement. Dans notre exemple, choisissez de **Créer un domaine dans une nouvelle forêt**. À noter que l'assistant vous indique un lien vers le fichier d'aide Windows traitant des différentes configurations de déploiement possibles.

© ENI Editions - All rigths reserved


Assistant Installation des services de domaine Active Directory
Choisissez une configuration de déploiement
Vous pouvez créer un contrôleur de domaine pour une forêt nouvelle ou existante.
Forêt existante
Ajouter un contrôleur de domaine à un domaine existant
Créer un nouveau domaine dans une forêt existante
Ce serveur va devenir le premier contrôleur de domaine du nouveau domaine.
Créer une nouvelle racine d'arborescence de domaine au lieu d'un nouveau domaine enfant
Créer un domaine dans une nouvelle forêt
En savoir plus sur les configurations de déploiement possibles
< Précédent
Suivant >
Annuler

Si vous avez choisi d'ajouter un contrôleur de domaine à un domaine existant, vous aurez la possibilité de définir l'installation du contrôleur de domaine à partir d'un média (une sauvegarde par exemple). C'est assez utile sur un site distant par exemple, afin d'éviter qu'un trafic réseau important ne vienne saturer la bande passante lors de la première synchronisation entre les contrôleurs de domaine. Vous pouvez sinon définir un contrôleur de domaine particulier pour la première synchronisation de l'annuaire Active Directory afin d'indiquer un contrôleur de domaine du même site et ainsi éviter que la synchronisation ne s'opère vers un site distant ayant une bande passante limitée.

- Nommez le domaine racine de la forêt. Dans notre exemple, le nom de domaine sera **masociete.local**.

  Il est toujours conseillé d'indiquer un nom de domaine à deux niveaux ; ne créez donc pas de domaine Active Directory ayant par exemple pour nom *Masociete*.

  Évitez également de définir un nom de domaine public type *masociete.com* ou *masociete.fr*. Cela entraînera en effet une gestion un peu plus complexe de votre zone DNS interne. Cliquez sur **Suivant**. L'assistant tentera alors de résoudre ce nom de domaine afin de contacter une éventuelle forêt existante.

Vous trouverez plus d'informations sur les différents types de zone DNS et sur la réplication dans le chapitre Mise en place des services réseaux d'entreprise - Mise en place des systèmes de résolution de nom.

- Laissez le nom de domaine NETBIOS par défaut et cliquez sur **Suivant**.

- Le niveau fonctionnel de la forêt devra alors être défini. Choisissez **Windows Server 2008**. Cela vous permettra en effet d'éviter d'avoir à augmenter le niveau fonctionnel de domaine des éventuels futurs domaines de cette même forêt.

  Vous profiterez ainsi automatiquement des avantages liés au niveau fonctionnel de domaine Windows Server 2008, comme les stratégies de mot de passe affinées (que vous verrez plus tard dans ce chapitre).

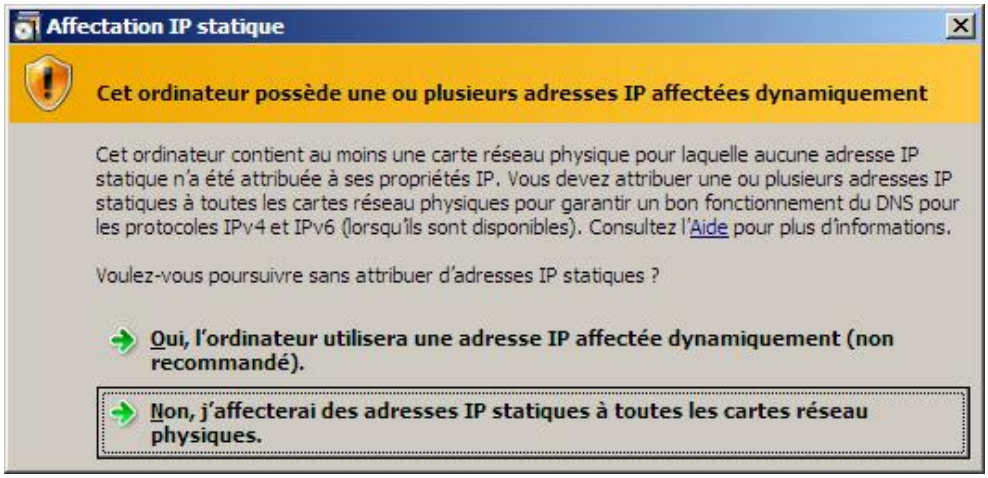
  Il faut savoir que le niveau fonctionnel de la forêt ne peut pas être mis à jour vers un niveau fonctionnel inférieur (Windows 2000 ou Windows 2003). Comme indiqué par l'assistant, vous ne pourrez ajouter à cette forêt que des contrôleurs de domaine exécutant Windows Server 2008 ou ultérieur.

  Cliquez sur **Suivant**.

© ENI Editions - All rigths reserved

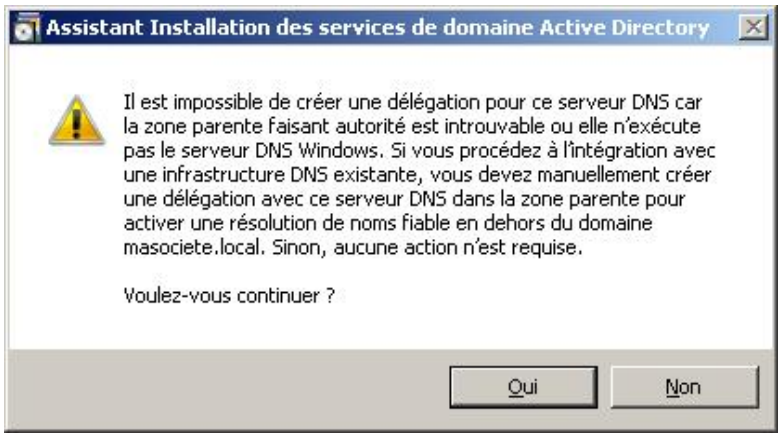
- Laissez la case **Serveur DNS** cochée afin d'installer ce rôle sur le futur contrôleur de domaine et cliquez sur **Suivant**. L'option **Catalogue Global** est forcément cochée dans notre exemple car aucun catalogue global n'existe encore sur le domaine puisque vous avez choisi de créer un nouveau domaine dans une nouvelle forêt.

Si vous n'avez pas défini d'adresse IP fixe à vos deux protocoles IPv4 et IPv6, le message suivant apparaîtra :


Affectation IP statique
Cet ordinateur possède une ou plusieurs adresses IP affectées dynamiquement
Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Vous devez attribuer une ou plusieurs adresses IP statiques à toutes les cartes réseau physiques pour garantir un bon fonctionnement du DNS pour les protocoles IPv4 et IPv6 (lorsqu'ils sont disponibles). Consultez l'Aide pour plus d'informations.
Voulez-vous poursuivre sans attribuer d'adresses IP statiques ?
Oui, l'ordinateur utilisera une adresse IP affectée dynamiquement (non recommandé).
Non, j'affecterai des adresses IP statiques à toutes les cartes réseau physiques.

Si vous ne prévoyez pas d'utiliser le protocole IPv6, il est conseillé de désinstaller celui-ci.

Le système tente alors de contacter le serveur DNS défini au niveau des paramètres TCP/IP de la carte réseau du serveur. Si celui-ci ne répond pas au nom de domaine Active Directory défini, et si aucun serveur DNS n'est installé, l'assistant affichera le message suivant :


Assistant Installation des services de domaine Active Directory
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine masociete.local. Sinon, aucune action n'est requise.
Voulez-vous continuer ?
Oui
Non

À noter également que si un serveur DNS est défini dans les propriétés TCP/IP du serveur, celui-ci sera automatiquement supprimé de ces propriétés de sorte que le futur contrôleur de domaine soit client de son propre DNS. L'ancien serveur DNS auparavant défini sera renseigné dans l'onglet **Redirecteurs des propriétés du service DNS**.

- Choisissez **Oui**.

- Comme vous vous trouvez dans un environnement de test, laissez le chemin par défaut pour la base de données, les fichiers journaux et SYSVOL. Dans un environnement de production, il est fortement conseillé de séparer la base de données et les fichiers journaux afin d'éviter la saturation des I/O (Entrées/Sorties). Cliquez sur **Suivant**.

- Définissez le mot de passe administrateur de restauration des services d'annuaire. Il vous sera utile en cas de restauration du serveur lors d'un démarrage en mode **Restauration des services d'annuaires** accessible via la touche [F8] au démarrage de votre système d'exploitation. Ce mot de passe devra répondre à la complexité requise par la stratégie de mot de passe.

© ENI Editions - All rigths reserved

Bien que cela soit tentant, ne définissez pas le même mot de passe que celui du compte Administrateur actuel pour des raisons de sécurité.

- Cliquez sur **Suivant**.

Un résumé affiche les différents choix que vous avez faits durant les étapes de l'assistant. Il vous est possible d'exporter ces paramètres afin de pouvoir les réutiliser dans un fichier de réponse.

Vous pourrez ainsi facilement déployer d'autres contrôleurs de domaine tout en minimisant le risque d'erreurs lors de la configuration de ce rôle. La commande à utiliser sera alors `dcpromo /answer:NomDuFichierCrée`.

Si vous exécutez directement la commande `dcpromo`, le rôle **Service de Domaine Active Directory** sera automatiquement installé.

- Cliquez sur **Suivant**. L'assistant lance l'installation du rôle Contrôleur de domaine sur Windows Server 2008. Une fois son installation terminée, choisissez de redémarrer le serveur.

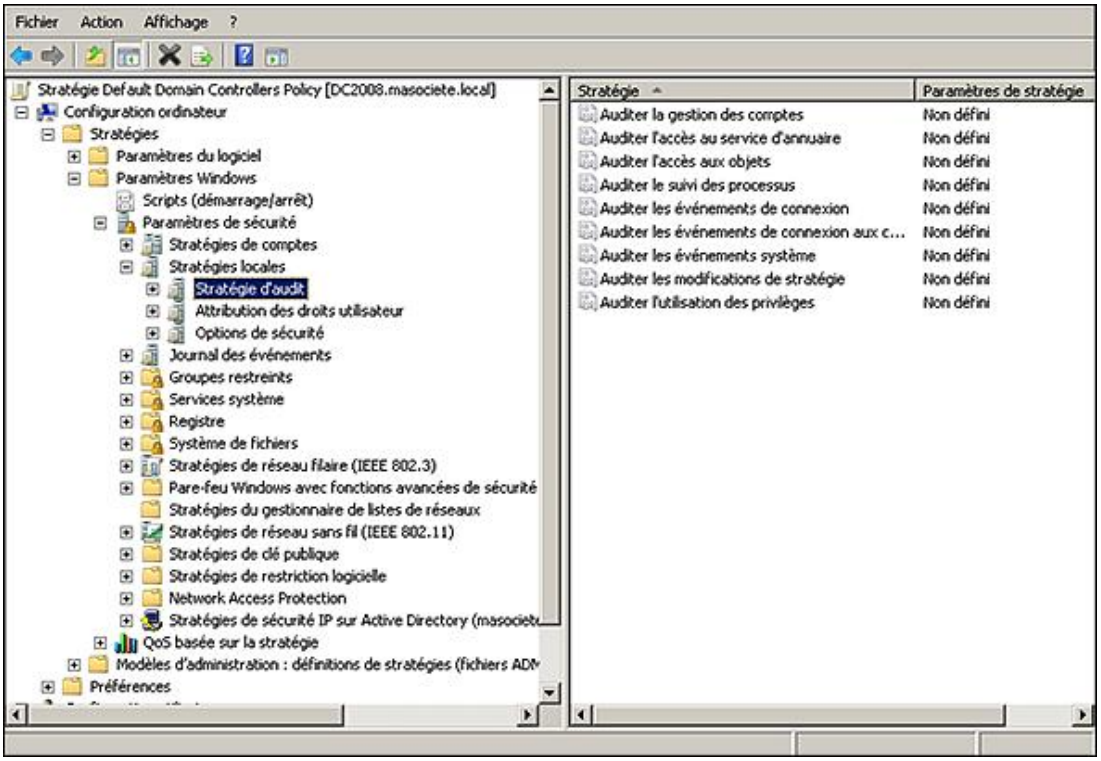
Lors du premier redémarrage du contrôleur de domaine, vous constaterez des messages d'avertissement liés aux rôles Serveur DNS et Services de domaine Active Directory. Ne vous inquiétez pas, ces messages peuvent être ignorés et disparaîtront rapidement d'eux-mêmes.

Félicitation ! Vous venez donc d'installer avec succès un contrôleur de domaine sous Windows Server 2008.

b. Présentation de l'audit lié au service d'annuaire

Auditer ses serveurs consiste à recenser les évènements que l'on juge intéressant dans le journal des évènements. Cela vous aide alors à mettre en évidence certains problèmes de configuration ou bien encore à vérifier la sécurité de certains éléments critiques du système d'exploitation. Attention cependant à ne pas définir trop d'objets à auditer car les performances du serveur en pâtiront immédiatement !

Sous Windows Server 2008, vous pourrez configurer les audits en éditant votre stratégie de groupe (depuis le menu **Démarrer** - **Outils d'administration** et **Gestion des stratégies de groupe**) au niveau de **Stratégie Default Domain Controllers Policy** (**Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Stratégies d'audit**).


Fichier Action Affichage ?
Stratégie Default Domain Controllers Policy [DC2008.masociete.local]
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Stratégie d'audit
Attribution des droits utilisateur
Options de sécurité
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 802.3)
Pare-feu Windows avec fonctions avancées de sécurité
Stratégies du gestionnaire de listes de réseaux
Stratégies de réseau sans fil (IEEE 802.11)
Stratégies de clé publique
Stratégies de restriction logicielle
Network Access Protection
QoS basée sur la stratégie
Préférences
Stratégie
Paramètres de stratégie
Auditer la gestion des comptes Non défini
Auditer l'accès au service d'annuaire Non défini
Auditer l'accès aux objets Non défini
Auditer le suivi des processus Non défini
Auditer les événements de connexion Non défini
Auditer les événements de connexion aux c... Non défini
Auditer les événements système Non défini
Auditer les modifications de stratégie Non défini
Auditer l'utilisation des privilèges Non défini

Les informations affichées sont cependant trompeuses !

© ENI Editions - All rigths reserved

Les stratégies d'audit peuvent en effet être définies de façon beaucoup plus fine désormais et les paramètres affichés au niveau de la stratégie de groupe ne représentent que très grossièrement la configuration effective.

En effet, afin d'afficher de façon plus fine les stratégies d'audit réellement définies, il vous faudra utiliser la ligne de commande suivante :

```
Auditpol.exe /get /Category :*
```

Administrateur : C:\Windows\system32\cmd.exe
C:\Users\Administrateur.DC2008>Auditpol.exe /get /Category:*
Stratégie d'audit système
Catégorie/Sous-catégorie Paramètre
Système
Extension système de sécurité Aucun audit
Intégrité du système Succès et échec
Pilote IPSEC Aucun audit
Autres événements système Succès et échec
Modification de l'état de la sécurité Opération réussie
Ouverture/Fermeture de session
Ouvrir la session Succès et échec
Fermer la session Opération réussie
Verrouillage du compte Opération réussie
Mode principal IPsec Aucun audit
Mode rapide IPsec Aucun audit
Mode étendu IPsec Aucun audit
Ouverture de session spéciale Opération réussie
Autres événements d'ouverture/fermeture de sessionAucun audit
Serveur de stratégie réseau Succès et échec
Accès aux objets
Système de fichiers Aucun audit
Registre Aucun audit
Objet de noyau Aucun audit
SAM Aucun audit
Services de certification Aucun audit
Généré par application Aucun audit
Manipulation de handle Aucun audit
Partage de fichiers Aucun audit
Rejet de paquet par la plateforme de filtrageAucun audit
Connexion de la plateforme de filtrage Aucun audit
Autres événements d'accès à l'objet Aucun audit
Utilisation d'un privilège
Utilisation de privilèges sensibles Aucun audit
Utilisation de privilèges non sensibles Aucun audit
Autres événements d'utilisation de privilègesAucun audit
Suivi détaillé
Fin du processus Aucun audit
Activité DPAPI Aucun audit
Événements RPC Aucun audit
Création du processus Aucun audit
Changement de stratégie
Auditer les modifications de stratégie Opération réussie
Modification de la stratégie d'authentificationOpération réussie
Modification de la stratégie d'autorisationAucun audit
Modification de la stratégie de niveau règle MPSSVCAucun audit
Modification de la stratégie de plateforme de filtrageAucun audit
Autres événements de modification de stratégieAucun audit
Gestion des comptes
Gestion des comptes d'utilisateur Opération réussie
Gestion des comptes d'ordinateur Opération réussie
Gestion des groupes de sécurité Opération réussie
Gestion des groupes de distribution Aucun audit
Gestion des groupes d'applications Aucun audit
Autres événements de gestion des comptesAucun audit
Accès DS
Modification du service d'annuaire Aucun audit
Réplication du service d'annuaire Aucun audit
Réplication du service d'annuaire détailléAucun audit
Accès Active Directory Opération réussie
Connexion de compte
Opérations de ticket du service KerberosOpération réussie

Vous remarquerez alors que les options d'audit sont beaucoup plus riches que sous les anciennes versions de Windows.

Les principales catégories ont été conservées et vous pourrez constater que beaucoup de sous-catégories viennent enrichir et rendre la collecte des évènements très précise.

Votre journal des évènements risquera donc d'être beaucoup moins pollué par des évènements inutiles.

Sachez toutefois que si vous utilisez la stratégie de groupe afin de définir les catégories principales d'audit, vous n'aurez pas la possibilité de définir de façon plus fine les paramètres des sous-catégories. Une stratégie d'audit configurée au niveau des stratégies de groupes active automatiquement les sous-catégories.

Si vous souhaitez toutefois pouvoir gérer la configuration des sous-catégories de vos Windows Vista/2008 de façon centralisée (et par conséquent sans avoir à passer par la commande `auditpol` sur chaque ordinateur), lisez l'excellente solution fournie dans l'article suivant de la KB Microsoft : http://support.microsoft.com/kb/921469

© ENI Editions - All rigths reserved

Une de ces nouvelles sous-catégories d'audit a été spécialement créée pour répondre à un besoin fort pour les administrateurs de domaine Active Directory.

Cette nouvelle sous-catégorie se nomme **Directory Service Changes** (catégorie enfant de DS Access). Elle vous permettra d'enregistrer les anciennes et les nouvelles valeurs attribuées à un objet Active Directory et à ses attributs. Pour information, auparavant, un contrôleur de domaine sous Windows 2000 ou 2003 indiquait simplement le nom de l'objet ou de l'attribut modifié mais non les anciennes et nouvelles valeurs de celui-ci.

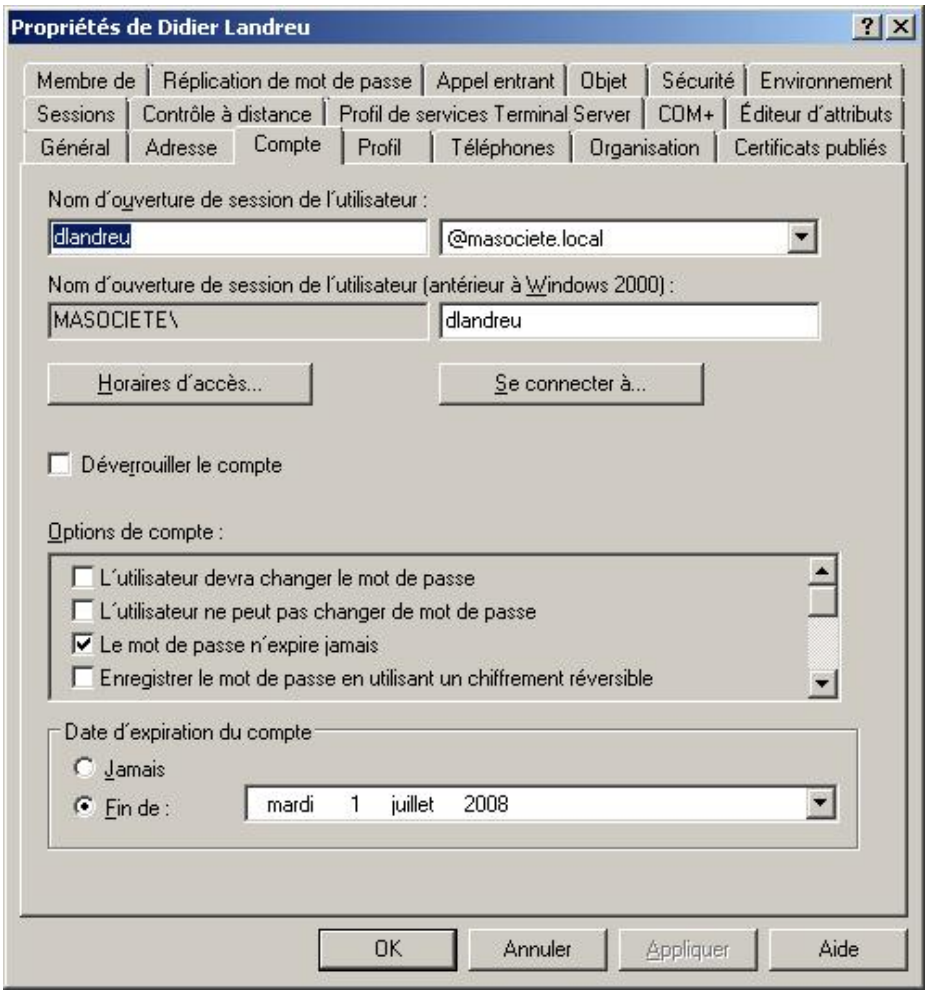
Une fois que l'audit de cette sous-catégorie aura été configuré, les évènements seront consignés dans le journal Sécurité. Le tableau suivant récapitule les quatre types d'évènements sur les objets Active Directory :

Numéro de l'évènement	Type de l'évènement
5136	Modification réussie d'un attribut de l'Active Directory.
5137	Création d'un nouvel objet de l'Active Directory.
5138	Restauration d'un objet de l'Active Directory.
5139	Déplacement d'un objet de l'Active Directory.

Si vous souhaitez par exemple activer l'audit pour toutes les sous-catégories concernant l'accès à l'annuaire Active Directory, suivez la procédure suivante :

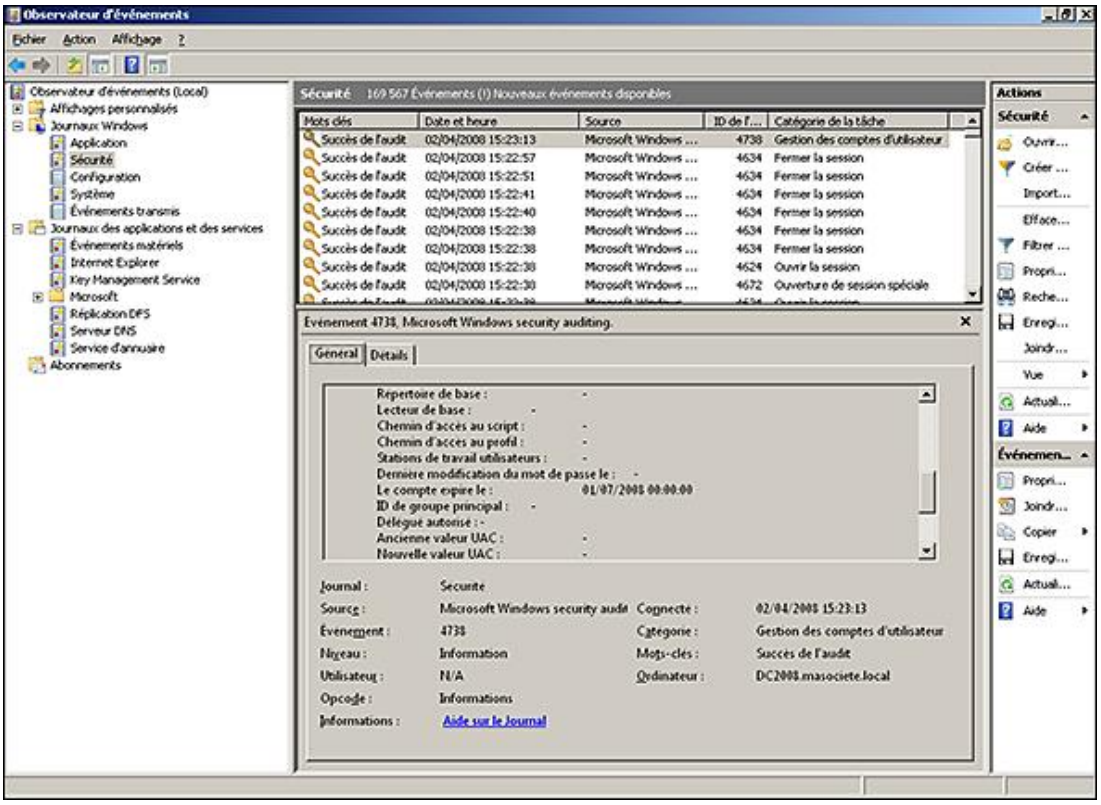
- La commande devra être exécutée sur le contrôleur de domaine : **Auditpol /set /category: " Accès DS" /success:enable**. Toutes les sous-catégories d'audit seront ainsi activées.

- Modifiez alors la date d'expiration d'un compte utilisateur de l'Active Directory via la console **Utilisateurs et ordinateurs Active Directory** (via **Démarrer - Exécuter - dsa.msc**).



© ENI Editions - All rigths reserved

- Ouvrez le journal des évènements de votre contrôleur de domaine (via **Démarrer - Exécuter - Eventvwr.msc**). Vous pouvez constater qu'un évènement 4738 est présent et qu'il précise la ou les valeurs qui viennent d'être modifiées ; dans notre exemple, la valeur **Le compte expire le :**.


Observateur d'événements
Fichier Action Affichage ?
Observateur d'événements (Local)
Affichages personnalisés
Journaux Windows
Application
Sécurité
Configuration
Système
Événements transmis
Journaux des applications et des services
Événements matériels
Internet Explorer
Key Management Service
Microsoft
Réplication DFS
Serveur DNS
Service d'annuaire
Abonnements
Sécurité 169 567 Événements (!) Nouveaux événements disponibles
Mots clés Date et heure Source ID de l'... Catégorie de la tâche
Succès de l'audit 02/04/2008 15:23:13 Microsoft Windows ... 4738 Gestion des comptes d'utilisateur
Succès de l'audit 02/04/2008 15:22:57 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:51 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:41 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:40 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:38 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:38 Microsoft Windows ... 4634 Fermer la session
Succès de l'audit 02/04/2008 15:22:38 Microsoft Windows ... 4624 Ouvrir la session
Succès de l'audit 02/04/2008 15:22:30 Microsoft Windows ... 4672 Ouverture de session spéciale
Événement 4738, Microsoft Windows security auditing.
General Details
Répertoire de base :
Lecteur de base :
Chemin d'accès au script :
Chemin d'accès au profil :
Stations de travail utilisateurs :
Dernière modification du mot de passe le :
Le compte expire le : 01/07/2008 00:00:00
ID de groupe principal :
Délégué autorisé :
Ancienne valeur UAC :
Nouvelle valeur UAC :
Journal : Sécurité
Source : Microsoft Windows security audit Connecté : 02/04/2008 15:23:13
Événement : 4738 Catégorie : Gestion des comptes d'utilisateur
Niveau : Information Mots-clés : Succès de l'audit
Utilisateur : N/A Ordinateur : DC2008.masociete.local
Opcode : Informations
Informations : Aide sur le Journal
Actions
Sécurité
Ouvrir...
Créer...
Importer...
Effacer...
Filtrer...
Propri...
Reche...
Enregi...
Joindr...
Vue
Actuali...
Aide
Événemen...
Propri...
Joindr...
Copier
Enregi...
Actuali...
Aide

c. Contrôleur de domaine en lecture seule

Windows Server 2008 permet de créer des **contrôleurs de domaine en lecture seule** (appelés aussi **RODC** pour *Read Only Domain Controller*). Un contrôleur de domaine en lecture seule contient toutes les informations d'un contrôleur de domaine classique à l'exception du mot de passe des utilisateurs. Ces informations sont stockées en lecture seule uniquement et aucune modification au niveau du domaine ne peut donc être initiée depuis un RODC.

Sachez d'ailleurs que si vous ne souhaitez pas la réplication d'un attribut jugé sensible sur vos RODC, il est possible de modifier les propriétés de celui-ci afin de limiter sa réplication uniquement à des contrôleurs de domaine inscriptibles. Pour cela, il vous faudra modifier la valeur **searchFlags** de l'attribut de votre choix au niveau de la partition de schéma. Le rôle maître de schéma devra d'ailleurs de préférence se trouver sur un contrôleur de domaine sous Windows Server 2008. Vous trouverez plus d'informations à ce sujet sur le lien suivant : http://technet2.microsoft.com/windowsserver2008/en/library/f62c9720-a5c3-40c9-aa40-440026f585e91033.mspx?mfr=true (en anglais)

Microsoft a donc réfléchi à une solution adaptée aux besoins des sociétés possédant des sites distants de quelques utilisateurs pour :

- augmenter la sécurité de ces sites ;
- améliorer l'authentification des utilisateurs d'un site distant sans forcément nécessiter un trafic WAN avec le contrôleur de domaine du site principal ;
- accéder aux ressources du réseau plus rapidement.

Augmenter la sécurité de ces sites

Auparavant, il était en effet nécessaire d'installer un contrôleur de domaine supplémentaire sur des sites distants si vous ne vouliez pas que certains utilisateurs se plaignent de lenteur d'authentification ou d'accès à des ressources du domaine. Le problème qui pouvait alors se poser était que ces sites n'avaient pas forcément les moyens ou le besoin d'avoir un administrateur à temps plein, ni d'investir dans un local protégé pour sécuriser leur serveur. En cas de vol ou de corruption du contrôleur de domaine de ce site, l'attaquant pouvait potentiellement récupérer tous les

© ENI Editions - All rigths reserved

noms d'utilisateurs et mots de passe des utilisateurs de la société.

Désormais, il est possible de limiter les conséquences d'une corruption d'un contrôleur de domaine sur ces sites car vous pouvez définir avec précision quels comptes ont leurs mots de passe stockés sur ce contrôleur de domaine en lecture seule. Cela se fait au travers de l'appartenance à deux groupes de sécurité appelés **Groupe de réplication dont le mot de passe RODC est autorisé** (mot de passe répliqué sur le RODC) et **Groupe de réplication dont le mot de passe RODC est refusé** (mot de passe non répliqué sur le RODC). Vous n'avez alors plus qu'à choisir les comptes de vos quelques utilisateurs et les ajouter au groupe de votre choix. En cas de conflit (si l'utilisateur appartient aux deux groupes précédents par exemple), le droit « Refusé » est prioritaire. Par défaut, deux condensés de mot de passe sont stockés sur un RODC. Celui du compte krbtgt_xxxx et celui du compte ordinateur. Le compte krbtgt_xxxx est propre à chaque RODC. Il permet de délivrer les tickets Kerberos aux clients en faisant la demande. En cas de vol du contrôleur de domaine d'un site, il vous suffit de réinitialiser les mots de passe de ces quelques comptes, comme vous le verrez plus bas.

Améliorer l'authentification des utilisateurs

Un RODC tente d'authentifier un compte par rapport aux mots de passe qu'il possède en cache. Si celui-ci ne se trouve pas dans son cache, il contactera un contrôleur de domaine inscriptible afin d'authentifier l'utilisateur. Dans le même temps, il regardera si la stratégie de réplication des mots de passe autorise le mot de passe de ce compte à être mis en cache sur le RODC ou non. Ainsi, si la stratégie le permet, les requêtes d'authentification seront directement traitées par le RODC.

Accéder aux ressources du réseau plus rapidement

Parmi les autres spécificités d'un contrôleur de domaine en lecture seule, sachez que ce dernier ne peut, par nature, que recevoir le trafic de réplication entrant (réplication unidirectionnelle). Il ne peut donc pas être défini comme serveur tête de pont d'une stratégie de réplication du domaine dans la mesure où il ne fait que subir les modifications sans pouvoir les initier.

Il est également possible d'installer le service DNS sur le RODC d'un site. Cela évite des temps de latence répétitifs lors de la tentative de résolution de nom par un utilisateur n'ayant pas de serveur DNS proche de lui. Ce service sera également en lecture seule sur un RODC et les ordinateurs n'auront pas la possibilité d'inscrire leurs enregistrements de façon dynamique sur ce DNS. Leurs requêtes d'inscription seront alors redirigées vers un DNS inscriptible.

Parmi les pré-requis à l'installation d'un RODC, sachez que :

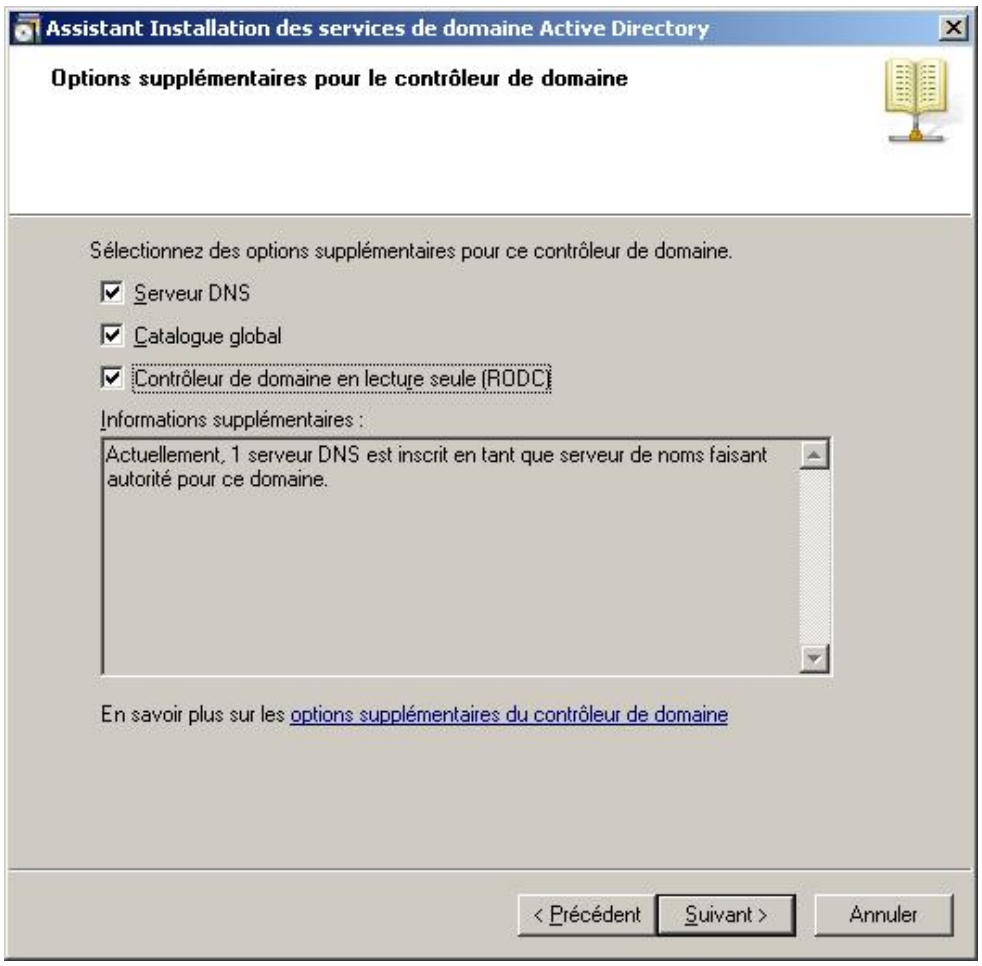
- Le contrôleur de domaine doit être capable de transférer les requêtes d'authentification vers un contrôleur de domaine sous Windows Server 2008.
- Le niveau fonctionnel de la forêt et du domaine doivent être configurés en *Windows Server 2003 ou plus*.
- La commande `adprep /rodcprep` doit être lancée une seule fois sur la forêt. Elle permet de mettre à jour l'ensemble des domaines de la forêt afin de modifier les permissions sur la partition d'annuaire de l'application DNS.

Procédez comme suit si vous souhaitez installer un contrôleur de domaine en lecture seule :

- L'installation d'un RODC est quasiment identique à la procédure que vous avez utilisée lors de l'installation d'un contrôleur de domaine classique. Après avoir choisi le serveur qui servira de RODC, ouvrez donc la console **Gestionnaire de serveur** puis **Ajouter des rôles**. Choisissez **Services de domaine Active Directory**. Les étapes suivantes de l'assistant se mettent à jour en fonction du rôle choisi. Cliquez alors sur **Suivant** puis **Installer**.
- Une fois le rôle installé, choisissez **Fermez cet Assistant et lancez l'Assistant Installation des services de domaine Active Directory (dcpromo.exe)**, cochez alors la case **Utiliser l'installation en mode avancé** sans quoi un contrôleur de domaine inscriptible sera installé sans que vous ayez la possibilité d'indiquer que celui-ci soit en lecture seule.
- Dans notre exemple, vous souhaitez installer un RODC, il vous faudra donc choisir d'installer un contrôleur de domaine **Dans une forêt existante et Ajoutez un contrôleur de domaine à un domaine existant**. Cliquez sur **Suivant**.
- Indiquez alors le nom du domaine existant sur lequel vous souhaitez ajouter un RODC puis cliquez sur **Définir** afin de spécifier le mot de passe d'un compte administrateur du domaine ou de l'entreprise. Cliquez alors sur **Suivant** (si une erreur apparait, c'est que votre configuration DNS doit avoir un souci ou que des ports réseaux sont à autoriser car votre serveur RODC n'arrive pas à contacter votre domaine). Sélectionnez le domaine puis cliquez sur **Suivant**.
- Sélectionnez le site Active Directory puis cliquez sur **Suivant**.

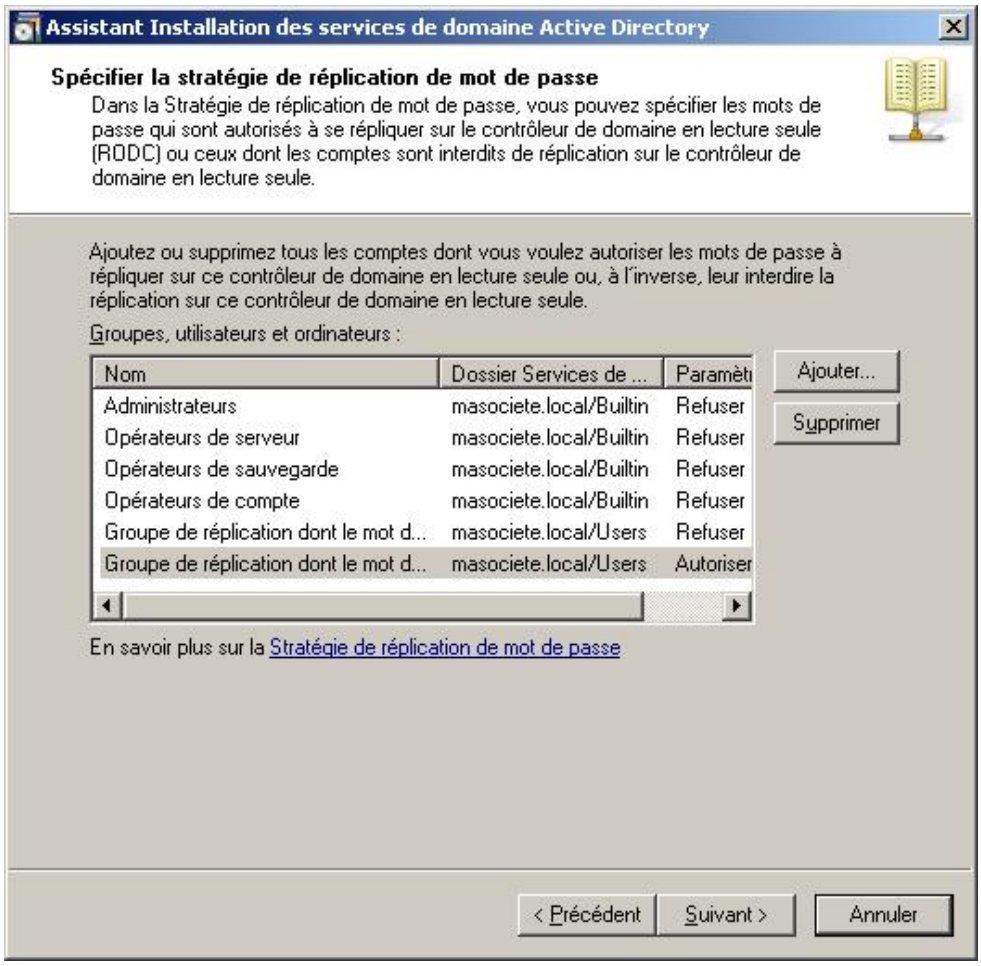
© ENI Editions - All rigths reserved

- À cette étape, cochez la case **Contrôleur de domaine en lecture seule (RODC)**. Si vous le souhaitez, vous pourrez attribuer le rôle de DNS et de catalogue global à ce futur contrôleur de domaine (en ayant toujours en tête les limitations énoncées précédemment). Cliquez sur **Suivant**.


Assistant Installation des services de domaine Active Directory
Options supplémentaires pour le contrôleur de domaine
Sélectionnez des options supplémentaires pour ce contrôleur de domaine.
Serveur DNS
Catalogue global
Contrôleur de domaine en lecture seule (RODC)
Informations supplémentaires :
Actuellement, 1 serveur DNS est inscrit en tant que serveur de noms faisant autorité pour ce domaine.
En savoir plus sur les options supplémentaires du contrôleur de domaine
< Précédent
Suivant >
Annuler

- Spécifiez alors la **Stratégie de réplication de mot de passe** en ajoutant ou supprimant les groupes et comptes utilisateurs qui seront autorisés ou refusés à répliquer leur mot de passe avec ce contrôleur de domaine en lecture seule. Une fois la réplication définie, cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Assistant Installation des services de domaine Active Directory
Spécifier la stratégie de réplication de mot de passe
Dans la Stratégie de réplication de mot de passe, vous pouvez spécifier les mots de passe qui sont autorisés à se répliquer sur le contrôleur de domaine en lecture seule (RODC) ou ceux dont les comptes sont interdits de réplication sur le contrôleur de domaine en lecture seule.
Ajoutez ou supprimez tous les comptes dont vous voulez autoriser les mots de passe à répliquer sur ce contrôleur de domaine en lecture seule ou, à l'inverse, leur interdire la réplication sur ce contrôleur de domaine en lecture seule.
Groupes, utilisateurs et ordinateurs :
Nom
Dossier Services de ...
Paramètr
Ajouter...
Supprimer
Administrateurs masociete.local/Builtin Refuser
Opérateurs de serveur masociete.local/Builtin Refuser
Opérateurs de sauvegarde masociete.local/Builtin Refuser
Opérateurs de compte masociete.local/Builtin Refuser
Groupe de réplication dont le mot d... masociete.local/Users Refuser
Groupe de réplication dont le mot d... masociete.local/Users Autoriser
En savoir plus sur la Stratégie de réplication de mot de passe
< Précédent
Suivant >
Annuler

- L'étape suivante permet de déléguer l'administration du RODC à l'utilisateur ou au groupe de votre choix. Dans la pratique, les membres de ce groupe se trouvent sur le site distant hébergeant ce contrôleur de domaine en lecture seule. Cliquez sur **Définir** pour ajouter le compte ou groupe de votre choix. Une fois l'ajout effectué, cliquez sur **Suivant**.

- Dans cette démonstration, vous choisirez **Répliquer les données sur le réseau à partir d'un contrôleur de domaine existant**. Cliquez sur **Suivant**.

- Si vous n'avez pas de contraintes particulières, laissez l'assistant choisir depuis quel contrôleur de domaine sera initié la réplication. Cliquez sur **Suivant**.

- Choisissez un répertoire de destination pour les fichiers de l'Active Directory. Afin d'améliorer les performances, la base de données Active Directory et les fichiers de logs ne doivent pas se trouver sur les mêmes disques durs. Une fois les répertoires choisis, cliquez sur **Suivant**.

- Définissez alors le mot de passe du compte Administrateur qui sera utilisé lors du redémarrage du contrôleur de domaine en mode **Restauration des services d'annuaire**.

- Un résumé vous informe alors des différents choix que vous avez faits à la suite du lancement de l'assistant. Vous pouvez également sauvegarder cette configuration en cliquant sur **Exporter les paramètres**. Le fichier de réponse créé permettra l'installation d'un RODC en ligne de commande et sans intervention de l'utilisateur (à noter que le mot de passe de restauration du service d'annuaire ne sera pas automatiquement sauvegardé dans le fichier créé. Il faudra indiquer celui-ci avant d'utiliser le fichier d'installation sans quoi l'assistant vous demandera de saisir le mot de passe au moment voulu). Cliquez sur **Suivant** afin de lancer l'installation puis sur **Terminer**. Redémarrez alors le serveur afin que les modifications puissent être prises en compte.

Le RODC est désormais installé. Vous devez maintenant configurer la **stratégie de réplication de mot de passe** depuis un contrôleur de domaine inscriptible. En effet, lorsqu'un RODC reçoit une demande d'authentification, il interroge la stratégie de réplication de mot de passe afin de déterminer s'il doit ou non garder en mémoire le mot de passe de l'utilisateur (ou de l'ordinateur) qui vient de s'authentifier. Par défaut, aucun mot de passe n'est gardé en mémoire. Suivant vos besoins, vous choisirez donc une stratégie de réplication de mot de passe plus ou moins sévère.

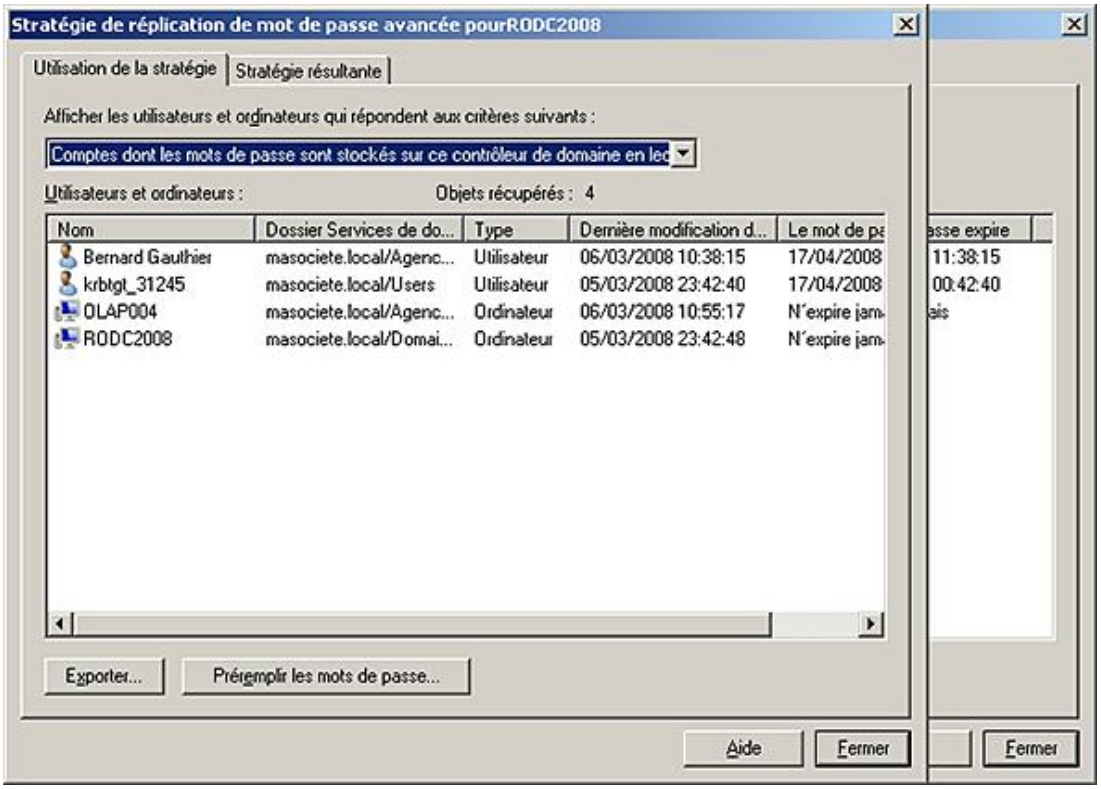
© ENI Editions - All rigths reserved

Afin de définir une stratégie de réplication de mot de passe, faites ce qui suit depuis un contrôleur de domaine (non-RODC).

- Cliquez sur **Démarrer - Outils d'administration**, et ouvrez la console **Utilisateurs et ordinateurs Active Directory**. Rendez-vous au niveau de l'unité d'organisation **Domain Controllers** et cliquez avec le bouton droit de la souris sur le contrôleur de domaine en lecture seule puis **Propriétés**.

- Cliquez sur l'onglet **Stratégie de réplication de mot de passe**. Comme expliqué précédemment, un RODC ne stocke les mots de passe que des comptes utilisateurs ou groupes qui sont définis comme **Autoriser** (pour autorisés à avoir leur mot de passe répliqué sur un RODC). Par défaut, la réplication du mot de passe est refusée pour les comptes d'administration comme Opérateurs de compte, Opérateurs de sauvegarde, Administrateurs, etc. **Ajouter** le compte de votre choix et choisissez si son mot de passe sera autorisé ou refusé à être répliqué sur ce RODC puis cliquez sur **OK** afin de choisir le compte utilisateur ou groupe sur votre domaine. Validez en cliquant sur **OK** à nouveau.

- Si vous cliquez sur le bouton **Avancé** vous pourrez afficher le nom des **Comptes dont les mots de passe sont stockés sur ce contrôleur de domaine en lecture seule**.



- Vous pouvez également choisir dans la liste déroulante d'afficher les **Comptes authentifiés sur ce contrôleur de domaine en lecture seule**. Il est en effet intéressant de savoir qui s'est authentifié en passant par ce RODC et ainsi modifier la stratégie de réplication de mot de passe pour mettre en cache le mot de passe de cet utilisateur et ainsi éviter des requêtes inutiles vers un contrôleur de domaine inscriptible. Vous pourrez également choisir de **Préremplir les mots de passe** des comptes. Cela peut s'avérer très utile si vous installez votre RODC depuis votre site principal et que vous préremplissez les mots de passe à mettre en cache des utilisateurs du site secondaire (sur lequel le RODC sera ensuite déplacé). Il faudra également préremplir les comptes ordinateurs utilisés par les utilisateurs ajoutés. Cela évitera d'avoir nécessairement la connexion WAN active entre les deux sites lors de la première authentification des utilisateurs sur le site secondaire. Bien entendu, les comptes choisis devront au préalable être ajoutés à la stratégie de réplication de mot de passe, sans quoi le refus implicite interdira la mise en cache du mot de passe.

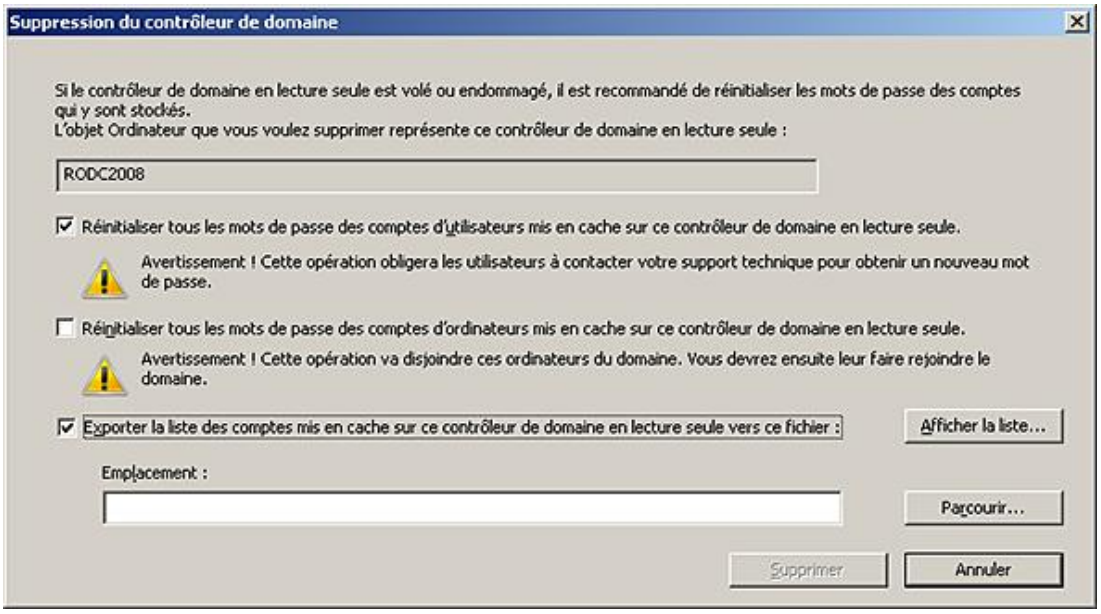
Sachez qu'il est possible de préremplir les mots de passe en utilisant la ligne de commande suivante : `repadmin /rodcpwdrepl [DSA_List] <Hub DC> <User1 Distinguished Name> [<Computer1 Distinguished Name> <User2 Distinguished Name> …]`. Exemple : si on veut pré-peupler le mot de passe du compte utilisateur Freddy ELMALEH (et de son ordinateur portable LAP_FEL) sur un RODC nommé RODCSrv01 depuis un contrôleur de domaine inscriptible nommé DCSrv02, la commande utilisée sera : `Repadmin /rodcpwdrepl RODCSrv01 DCSrv02 "CN=FreddyELMALEH,OU=Utilisateurs_IT,DC=masociete,DC=local" "CN=LAP_FEL,OU=Ordinateurs_IT,DC=masociete,DC=local"`.

© ENI Editions - All rigths reserved

En cas de vol d'un RODC, vous pouvez très aisément contrôler les comptes impactés et ainsi limiter les risques potentiels de sécurité dûs au vol de ce serveur. En tant qu'administrateur, voici comment vous devrez réagir face à une telle situation :

- Depuis un contrôleur de domaine inscriptible, cliquez sur **Démarrer - Outils d'administration**, et ouvrez la console **Utilisateurs et ordinateurs Active Directory**. Rendez-vous au niveau de l'unité d'organisation **Domain Controllers** et cliquez avec le bouton droit de la souris sur le compte ordinateur du contrôleur de domaine en lecture seule puis **Supprimer**. Confirmez la suppression en cliquant sur **Oui**.

- Une fenêtre s'affiche alors vous permettant de forcer la réinitialisation du mot de passe pour vos comptes utilisateurs et/ou ordinateurs. Il vous est également possible d'exporter la liste des comptes qui étaient mis en cache. Une fois vos options choisies, cliquez sur **Supprimer**.


Suppression du contrôleur de domaine
Si le contrôleur de domaine en lecture seule est volé ou endommagé, il est recommandé de réinitialiser les mots de passe des comptes qui y sont stockés.
L'objet Ordinateur que vous voulez supprimer représente ce contrôleur de domaine en lecture seule :
RODC2008
Réinitialiser tous les mots de passe des comptes d'utilisateurs mis en cache sur ce contrôleur de domaine en lecture seule.
Avertissement ! Cette opération obligera les utilisateurs à contacter votre support technique pour obtenir un nouveau mot de passe.
Réinitialiser tous les mots de passe des comptes d'ordinateurs mis en cache sur ce contrôleur de domaine en lecture seule.
Avertissement ! Cette opération va disjoindre ces ordinateurs du domaine. Vous devrez ensuite leur faire rejoindre le domaine.
Exporter la liste des comptes mis en cache sur ce contrôleur de domaine en lecture seule vers ce fichier :
Afficher la liste...
Emplacement :
Parcourir...
Supprimer
Annuler

Votre contrôleur de domaine RODC est alors supprimé et même si un attaquant tente d'exploiter les mots de passe stockés sur celui-ci, ces derniers n'auront plus d'utilités car ils auront été aisément et rapidement modifiés.

d. Stratégies de mot de passe et de verrouillage de compte granulaire

Une des principales améliorations attendues par les professionnels de l'informatique utilisant l'annuaire Microsoft est sans aucun doute la possibilité de pouvoir définir des stratégies de mot de passe multiples sur un domaine Active Directory. Il n'était en effet pas possible de faire cela dans les versions précédentes d'Active Directory.

Windows Server 2008 contient en effet une nouvelle classe d'objets nommée **msDS-PasswordSettings** qui rend possible la multiplication des stratégies de mot de passe au sein d'un même domaine. Sur un domaine Active Directory existant, il faudra mettre à jour le niveau fonctionnel du domaine en Windows Server 2008 (tous vos contrôleurs de domaine sur le domaine en question devront donc être sous Windows Server 2008).

Il est ainsi possible de définir un objet paramètres de mot de passe (appelé aussi PSO pour *Password Settings Object*) différent entre les utilisateurs. Dans la pratique, vous pourrez ainsi avoir une durée de vie maximale des mots de passe de 30 jours pour les comptes administrateurs. Les comptes de services auront quand à eux une longueur minimale du mot de passe de 36 caractères et qui n'expire jamais.

Par défaut, seuls les membres du groupe « Administrateurs du domaine » ont la possibilité de définir des stratégies de mot de passe multiples.

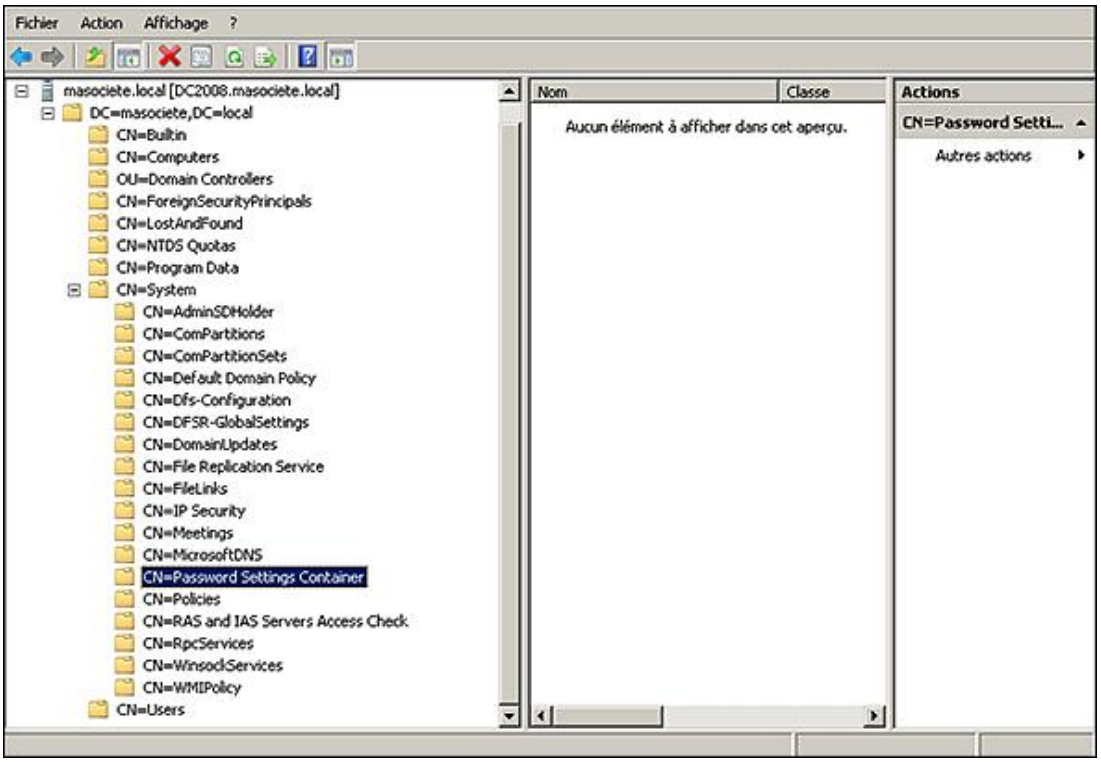
Prenons l'exemple de la définition d'une stratégie de mot de passe affinée pour les comptes utilisateurs utilisés pour l'administration du système d'information. Ces comptes utilisateurs font partis de groupes de sécurité leur octroyant beaucoup de droits sur le domaine et la compromission de leur mot de passe par un attaquant lui permettrait d'avoir un accès dangereux sur les serveurs. Il convient donc de sécuriser plus particulièrement ces comptes utilisateurs un peu spéciaux. Les paramètres de mot de passe seront les mêmes que ceux définis au niveau de la stratégie *Default Domain Policy* à la différence de la durée de vie maximale du mot de passe qui sera de 30 jours au lieu de 42 jours. La longueur minimale du mot de passe passera également de 7 à 14 caractères. Le compte sera également verrouillé après 10 mauvaises tentatives. Ces principes limitent les risques de compromissions du mot de passe des administrateurs. Afin de créer cette stratégie particulière, suivez les étapes suivantes :

- Ouvrez la console **adsiedit.msc** (depuis le menu **Démarrer - Exécuter** d'un Windows 2008 de préférence) avec un

© ENI Editions - All rigths reserved

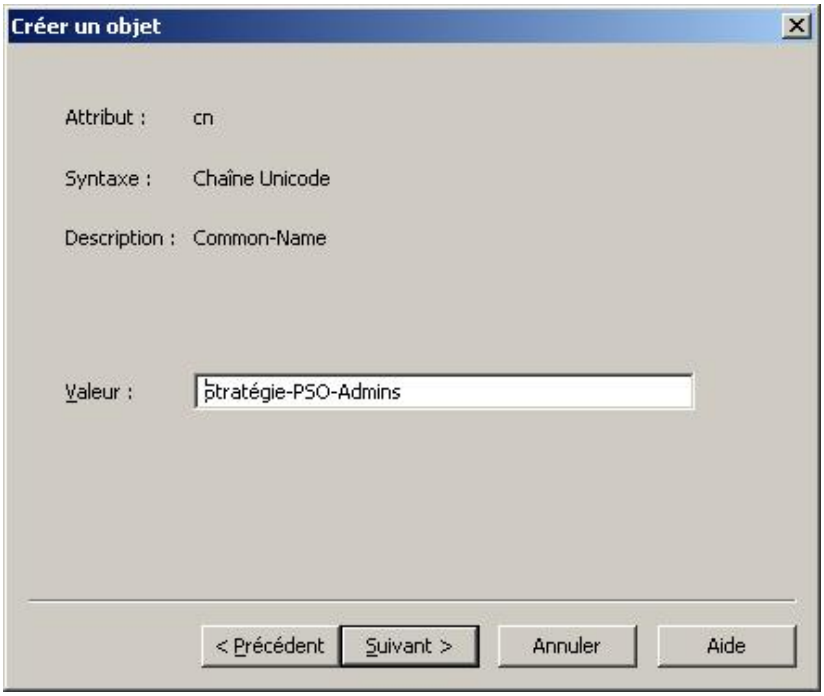
compte utilisateur membre du groupe « Admins du domaine ». Faites un clic avec le bouton droit sur **Modification ADSI**, puis **Connexion**.

- Dans **Nom** : indiquez le nom FQDN du domaine (dans notre exemple ***masociete.local***) puis cliquez sur **OK**. Naviguez alors dans l'arborescence sur la gauche de l'écran en cliquant sur ***Nom_FQDN_Du_Domaine*/CN=System/CN=Password Settings Container**. Faites un clic avec le bouton droit sur **CN=Password Settings Container** puis **Nouveau - Objet**.



- Dans **Créer un objet**, sélectionnez la classe **msDS-PasswordSettings** puis **Suivant**. Donnez un Common-Name à cet objet, comme *Stratégie-PSO-Admins* puis **Suivant**.

Cette stratégie sera appliquée à un groupe de sécurité nommé PSO-Admins. Ce groupe contiendra les utilisateurs pour lesquels vous souhaitez voir cette stratégie appliquée.



© ENI Editions - All rigths reserved

Vous devrez alors définir des valeurs pour un ensemble d'attributs.

- **msDS-PasswordSettingsPrecedence** correspond à une valeur de précédence. Elle doit avoir une valeur supérieure à 0 et permet l'arbitrage en cas de conflit lorsque deux objets PSO s'appliquent à un même utilisateur ou groupe. Deux règles sont à retenir si plusieurs paramètres s'appliquent à un même objet. L'objet PSO disposant de la valeur de précédence la plus faible sera appliqué et une stratégie appliquée au niveau Utilisateur sera prioritaire comparée à une stratégie appliquée au niveau Groupe.

Prévoyez d'espacer la numérotation de l'attribut **msDS-PasswordSettingsPrecedence** entre chaque stratégie PSO afin de vous permettre de jouer sur les priorités en cas de besoin futur.

- **msDS-PasswordReversibleEncryptionEnabled** est un booléen. Cet attribut correspond à l'option **Enregistrer les mots de passe en utilisant un chiffrement réversible**. Il est préférable d'indiquer la valeur **FALSE** sauf si vous avez des besoins particuliers.

- **msDS-PasswordHistoryLength** définit le nombre d'anciens mots de passe que l'utilisateur ne peut pas réutiliser. Il correspond au paramètre *Conserver l'historique des mots de passe*. Par défaut, sa valeur est de 24 sur le domaine.

- **msDS-PasswordComplexityEnabled** est un booléen qui définit si le mot de passe respecte des exigences de complexité ou non. **TRUE** est la valeur conseillée.

- **msDS-MinimumPasswordLength** est un entier qui définit *la longueur minimale du mot de passe*. La valeur par défaut est 7 sur le domaine. Dans notre exemple, il s'agit d'un PSO pour les comptes administrateurs. La valeur minimale sera donc indiquée à **14** caractères.

- **msDS-MinimumPasswordAge** est une durée qui indique *la durée de vie minimale du mot de passe* afin d'empêcher l'utilisateur de changer son mot de passe de façon successive jusqu'à ce qu'il dépasse la limite de l'historique des mots de passe afin de revenir sur son nouveau mot de passe. La valeur par défaut est de 1 jour. Son format s'inscrit alors ainsi **1:00:00:00**.

- **msDS-MaximumPasswordAge** est une durée qui indique *la durée de vie maximale du mot de passe*. Par défaut, le mot de passe doit être changé tous les 42 jours. Dans cet exemple, choisissez une durée de vie maximale de 30 jours soit **30:00:00:00**.

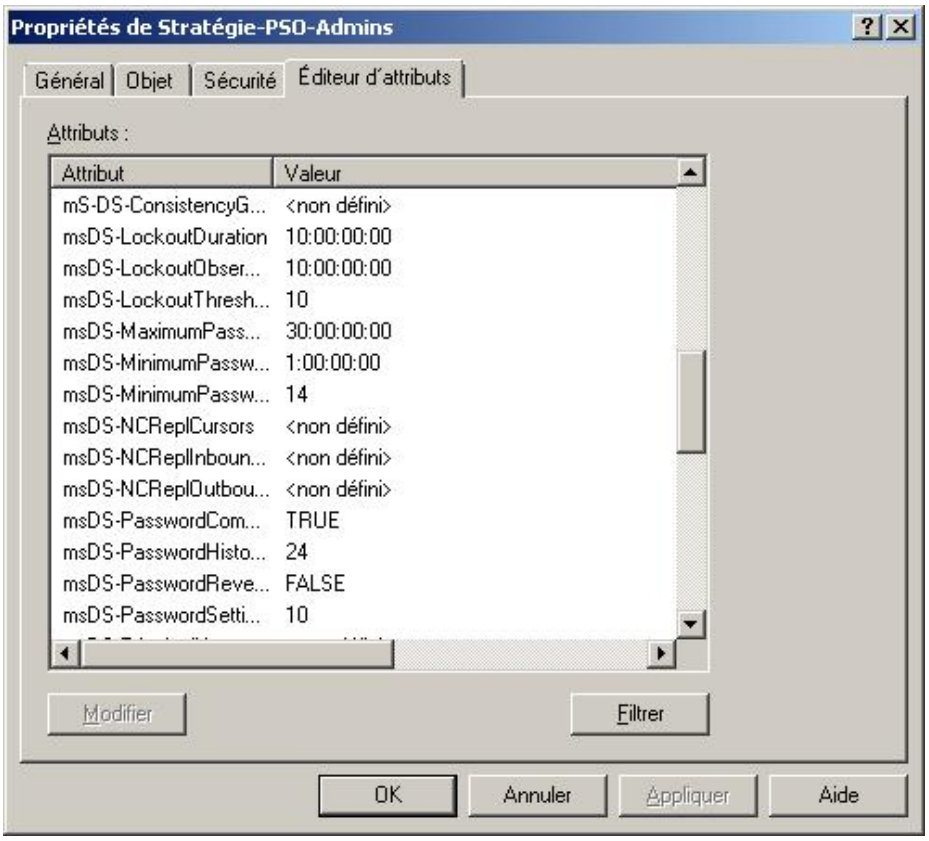
- **msDS-LockoutThreshold** définit le nombre de mots de passe erronés saisis avant que l'objet ne soit verrouillé. Il correspond au paramètre Seuil de verrouillage du compte qui est égal à 0 (ce qui indique que le compte n'est jamais verrouillé). Il est préférable d'indiquer un nombre de tentatives restreint pour éviter des attaques sur le mot de passe. Indiquez une valeur à **10** par exemple.

- **msDS-LockoutObservationWindows** permet de *Réinitialiser le compteur de verrouillages du compte après la* durée de votre choix. Indiquez une valeur de 10 minutes par exemple sous la forme **10:00:00:00**.

- **msDS-LockoutDuration** indique la *durée de verrouillage des comptes* en cas de X mauvais mots de passe saisis à plusieurs reprises (X représentant la valeur de msDS-LockoutThreshold). Indiquez une valeur de 10 minutes par exemple sous la forme **10:00:00:00**.

- Cliquez alors sur **Attributs Supplémentaires**, afin de lier cette stratégie à un utilisateur ou à un groupe. La liaison se fait au travers de l'attribut **msDS-PSOAppliesTo**, capable de contenir plusieurs valeurs (donc plusieurs utilisateurs et groupes). Choisissez ces paramètres : *Sélectionnez les propriétés à afficher* : **Les deux** et *Sélectionnez une propriété à afficher* : **msDS-PSOAppliesTo**. Dans modifier un attribut, indiquez le nom unique du groupe sous la forme **DN=PSO-Admins**, **OU=Admin-Groups**, **OU=Admins**, **OU=Paris**, **DC=masociete**, **DC=local**. Puis cliquez sur **Ajouter**. Vous pouvez ajouter autant de nom unique que vous le souhaitez. Une fois l'opération terminée, cliquez sur **OK**.

© ENI Editions - All rigths reserved



L'objet paramètres de mot de passe sera également accessible depuis la Console Utilisateurs et Ordinateurs Active Directory sur laquelle vous aurez affiché les **Fonctionnalités avancées** dans le menu **Affichage de la console**. L'objet est alors visible et modifiable depuis le conteneur **System/ Password Settings Container**.

Préférez appliquer une stratégie de mot de passe à un groupe plutôt qu'à un utilisateur afin de permettre une gestion bien plus simple et efficace. Si vous souhaitez connaître la stratégie appliquée à un utilisateur ou un groupe, affichez les propriétés du compte en question puis sélectionnez l'onglet **Éditeur d'attributs** puis **Filtrer**, **Affichez les attributs** : **Facultatif** et **Afficher les attributs en lecture seule : Construit**. L'attribut **msDS-ResultantPSO** sera alors visible et indiquera la stratégie PSO effective. Si l'attribut est nul alors la stratégie de mot de passe du domaine est appliquée pour le compte vérifié.

Vous pourrez utiliser des outils tiers gratuits afin de vous aider à la configuration des stratégies PSO. Il existe un très bon outil en ligne de commande nommé PSOMgr.exe disponible sur http://www.joeware.net ou bien encore un outil graphique facile à prendre en main qui s'appelle SpecOps Password Policy Basic disponible sur http://www.specopssoft.com.

---

e. Active Directory en tant que service Windows

Il est possible avec n'importe quel contrôleur de domaine sous Windows Server 2008 d'arrêter et de démarrer l'annuaire Active Directory car celui-ci est désormais considéré comme un service Windows.

Vous pouvez donc effectuer des opérations de maintenance comme la défragmentation hors-ligne de la base de données de l'annuaire Active Directory sans nécessairement redémarrer le serveur en mode Restauration du service d'annuaire.

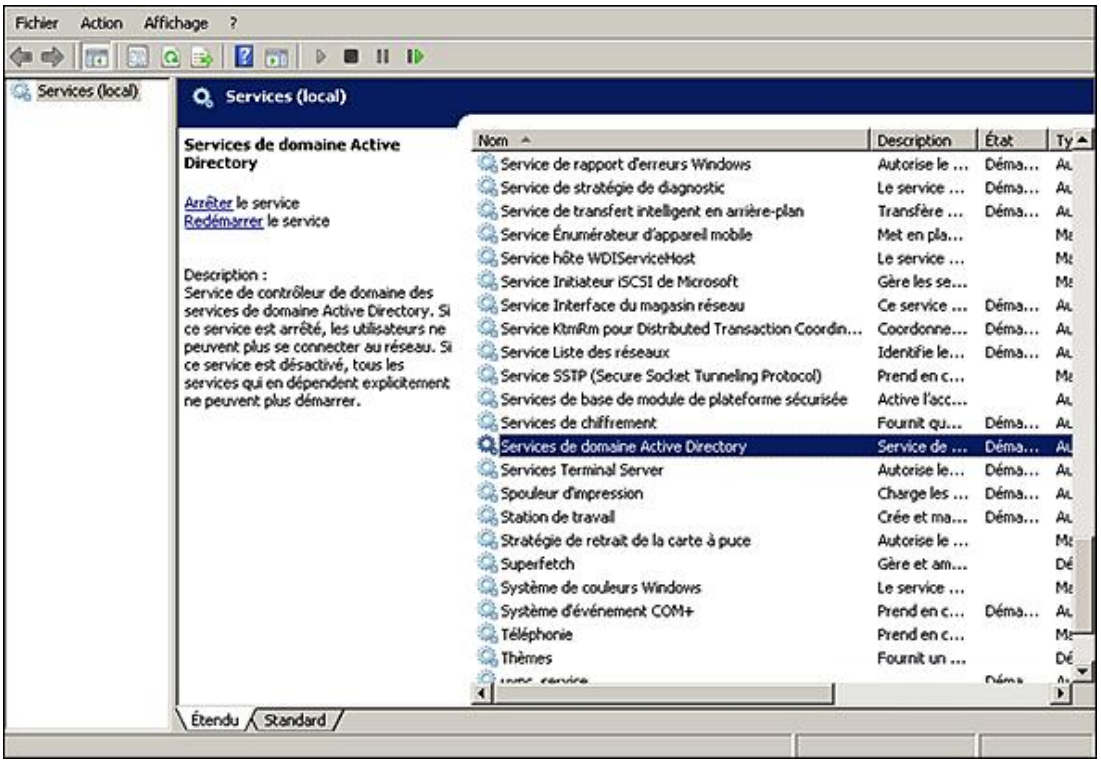
Les mises à jour Windows impactant le service d'annuaire ne nécessitent plus systématiquement le redémarrage complet du serveur. Un simple redémarrage du service Active Directory suffira.

Le principal avantage d'avoir rendu Active Directory en tant que service est que les autres services installés sur le contrôleur de domaine ne seront plus inaccessibles lorsqu'une opération de maintenance sera nécessaire.

La défragmentation de la base de données de l'annuaire Active Directory ne rendra donc plus nécessairement le service DHCP (installé sur ce même serveur) inaccessible.

Vous pouvez configurer l'état du service au niveau de la console MMC services, disponible depuis les outils d'administration ou en tapant **services.msc** dans **Exécuter**.

© ENI Editions - All rigths reserved


Fichier Action Affichage ?
Services (local)
Services de domaine Active Directory
Arrêter le service
Redémarrer le service
Description :
Service de contrôleur de domaine des services de domaine Active Directory. Si ce service est arrêté, les utilisateurs ne peuvent plus se connecter au réseau. Si ce service est désactivé, tous les services qui en dépendent explicitement ne peuvent plus démarrer.
Nom
Description
État
Service de rapport d'erreurs Windows
Service de stratégie de diagnostic
Service de transfert intelligent en arrière-plan
Service Énumérateur d'appareil mobile
Service hôte WDIServiceHost
Service Initiateur iSCSI de Microsoft
Service Interface du magasin réseau
Service KtmRm pour Distributed Transaction Coordin...
Service Liste des réseaux
Service SSTP (Secure Socket Tunneling Protocol)
Services de base de module de plateforme sécurisée
Services de chiffrement
Services de domaine Active Directory
Services Terminal Server
Spouleur d'impression
Station de travail
Stratégie de retrait de la carte à puce
Superfetch
Système de couleurs Windows
Système d'événement COM+
Téléphonie
Thèmes
Étendu
Standard

Le service apparaît sous le nom complet **Services de domaine Active Directory**. Le nom du service est **NTDS**.

Lorsque le statut du service est défini sur **Arrêté**, le contrôleur de domaine est vu par les autres ordinateurs comme un serveur membre du domaine sur lequel des stratégies de groupe peuvent être appliquées. Le contrôleur de domaine se comporte également comme s'il était en mode **Restauration de service d'annuaire**. Son fichier **ntds.dit** est libéré et si aucun contrôleur de domaine n'est joignable pour vous authentifier lors de l'ouverture de session, il vous faudra utiliser le mot de passe du compte administrateur de restauration des services d'annuaire défini lors de la promotion du serveur en tant que contrôleur de domaine.

f. Cliché instantané de l'Active Directory

Windows Server 2008 propose la création de clichés instantanés se reposant sur l'API VSS (*Volume Shadow Copy* ou Cliché Instantané de Volume). Pour vous aider dans vos recherches anglophones sur Internet, sachez que cette fonctionnalité s'appelle également Database Mounting Tool.

Le principal avantage est qu'une sauvegarde de ce type est possible même sur des fichiers verrouillés. Il n'est donc pas nécessaire d'arrêter le service Active Directory (et ainsi libérer les fichiers attachés) pour pouvoir sauvegarder le fichier **ntds.dit** par exemple.

Vous pouvez coupler l'utilisation du cliché instantané avec l'utilisation de l'outil **dsamain.exe** afin de mettre en évidence n'importe quel changement effectué dans l'Active Directory.

Par défaut, uniquement les utilisateurs membres du groupe Administrateurs du domaine et Administrateurs de l'entreprise sont autorisés à accéder aux clichés instantanés créés.

Afin d'utiliser au mieux les clichés instantanés pour l'Active Directory, trois outils sont indispensables.

- La commande `ntdsutil` pour créer, supprimer, lister, monter, démonter une sauvegarde (appelée pour l'occasion cliché instantané).
- La commande `dsamain` utilisée pour afficher le différentiel entre deux clichés instantanés par exemple.
- L'outil **ldp.exe** pour voir les données d'un cliché instantané de façon graphique.

L'utilisateur ne pourra accéder qu'aux données sauvegardées pour lesquelles les droits lui sont attribués. Les permissions sur les objets de la sauvegarde ne peuvent pas être modifiées car cette dernière est en lecture seule.

- Afin de créer un cliché instantané de l'annuaire Active Directory, vous allez utiliser la commande `ntdsutil`. Sachez toutefois que de nombreux autres logiciels du marché peuvent fonctionner à partir du moment où ces derniers utilisent la technologie des clichés instantanés.

© ENI Editions - All rigths reserved

La commande à utiliser est :

```
ntdsutil snapshot "activate instance ntds" create
```

- Vous pouvez planifier la sauvegarde de ces clichés via le planificateur de tâches. La commande à définir sera alors légèrement différente car vous devrez sortir du prompt ntdsutil.

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

- Une fois le cliché terminé, vous pouvez choisir d'afficher tous les clichés déjà créés. Si vous êtes déjà au niveau de l'invite *instantané* : , tapez uniquement **List All** (sinon la commande complète est `ntdsutil snapshot "activate instance ntds" "List All"`).

- Il vous faudra alors monter le cliché de votre choix afin de pouvoir lire les données qui y avaient été sauvegardées.

  mount *x* (ou x correspond au numéro du cliché instantané).

Une fois le cliché monté, tapez **quit** deux fois de suite afin de revenir à une invite de commande classique.

Administrateur : C:\Windows\system32\cmd.exe
C:\Users\Administrateur>ntdsutil snapshot "activate instance ntds" create
ntdsutil: snapshot
instantané : activate instance ntds
Instance active définie à « ntds ».
instantané : create
Création d'une capture instantanée...
Le jeu de captures instantanées {a777dbe5-ea9e-417e-ac47-d87be1c877f6} a été généré.
instantané : list all
1 : 2008/03/11:17:57 {66b89eb8-61a3-4e88-a546-9830f188ecd5}
2 : C: {aeb2a63c-b58e-41cb-a6fe-ce4513b9de66}
3 : 2008/03/11:17:57 {0bc7e366-a244-47f3-b511-daf051f532a6}
4 : C: {2692d303-86e3-487d-92c4-9c4c2903f4b0}
5 : 2008/03/11:23:33 {7f1c4c74-ed6b-4823-bebd-2bcbe44accc5}
6 : C: {972dd642-f3b0-491b-adef-66e8d0de1823}
7 : 2008/03/11:23:39 {f757407f-f3f0-4c12-99e1-dd441897583a}
8 : C: {12d65228-5503-47f1-9ce7-569facb0ec70}
9 : 2008/03/11:23:49 {a777dbe5-ea9e-417e-ac47-d87be1c877f6}
10 : C: {30627468-a8a7-4743-914f-e64545f7933f}
instantané : mount 7
Capture instantanée {12d65228-5503-47f1-9ce7-569facb0ec70} montée en tant que C:\$SNAP_200803112339_VOLUMEC$\
instantané : quit
ntdsutil: quit
C:\Users\Administrateur>_

Création d'un cliché instantané de l'annuaire Active Directory et montage d'une de ces sauvegardes.

- Maintenant il va falloir attacher cette sauvegarde à un serveur LDAP virtuel à l'aide de la commande `dsamain`.

  Pour cela, ouvrez une invite de commande avec un compte utilisateur membre du groupe Administrateurs du domaine ou Administrateurs de l'entreprise et tapez la commande suivante :

```
dsamain /dbpath < Chemin de la base de donnée AD > /ldapport <numéro de
port non utilisé>
```

Administrateur : C:\Windows\system32\cmd.exe - dsamain /dbpath C:\$SNAP_200803112339_VOLUMEC$\WINDOWS\NTDS\ntds.dit /ldapport 51389
C:\Users\Administrateur>ntdsutil snapshot "activate instance ntds" "list mounted" quit quit
ntdsutil: snapshot
instantané : activate instance ntds
Instance active définie à « ntds ».
instantané : list mounted
1 : 2008/03/11:23:39 {f757407f-f3f0-4c12-99e1-dd441897583a}
2 : C: {12d65228-5503-47f1-9ce7-569facb0ec70} C:\$SNAP_200803112339_VOLUMEC$\
instantané : quit
ntdsutil: quit
C:\Users\Administrateur>dsamain /dbpath C:\$SNAP_200803112339_VOLUMEC$\WINDOWS\NTDS\ntds.dit /ldapport 51389
EVENTLOG (Informational): NTDS General / Contrôle du service : 1000
Démarrage des services de domaine Microsoft Active Directory terminé, version 6.0.6001.18000

Si le domaine depuis lequel avait été créé le cliché instantané n'existe plus, il vous faut ajouter l'argument /**allowNonAdminAccess**. Si votre pare-feu est activé, il faudra créer une exception pour l'exécutable dsamain.exe.

© ENI Editions - All rigths reserved

- Votre serveur LDAP virtuel est maintenant accessible tant que vous laisserez l'invite de commande ouverte. Connectez-vous via un client capable d'accéder aux données de ce serveur LDAP. Dans cet exemple, vous utiliserez l'outil **ldp.exe** disponible par défaut dans Windows.

Depuis le menu **Démarrer - Exécuter**, tapez la commande `ldp.exe`. Cliquez alors sur **Connexion** et **Se connecter**. Dans l'adresse du serveur, tapez l'adresse IP du serveur et indiquez le port précédemment défini avec dsamain (ici 51389). Puis cliquez sur **OK**.

- Vérifiez le type de liaison via le menu **Connexion - Lier**. Assurez-vous de définir un compte utilisateur si celui qui est actuellement connecté ne possède pas les droits suffisants. Une fois configuré, cliquez sur **OK** afin de vous authentifier sur ce fichier d'annuaire.

- Cliquez alors sur **Affichage - Arborescence**, et définissez le nom unique de base correspondant à votre nom de domaine ; dans l'exemple, ce sera **DC=masociete, DC=local**.

Vous pouvez alors naviguer dans la sauvegarde de votre annuaire via cet outil.

Si vous trouvez que l'accès aux données n'est pas très digeste via l'outil **ldp.exe**, sachez que vous pourrez, si vos besoins sont plus limités, voir vos données directement depuis la console Utilisateurs et Ordinateurs Active Directory. Pour cela, faites un clic avec le bouton droit de la souris à la racine de la console puis choisissez **Changez de contrôleur de domaine**. Cliquez sur le message **<Tapez ici un nom de serveur d'annuaire :[port]>** pour y indiquer le nom de votre contrôleur de domaine et le port défini précédemment. Vous accéderez alors à votre annuaire de façon plus pratique qu'avec l'outil **ldp.exe**. Afin d'être complet, il ne faut pas oublier de citer le très bon outil ADExplorer (http://technet.microsoft.com/en-us/sysinternals/66963907.aspx). Il vous permettra de comparer aisément deux clichés instantanés (créés via cet outil), ce qui peut s'avérer extrêmement utile.

- Une fois terminé, n'oubliez pas de fermer dsamain ([Ctrl] **C** à deux reprises) et de démonter l'annuaire avec la commande `ntdsutil snapshot "activate instance ntds" "unmount x"` ou `x` est le numéro du cliché instantané.

g. Les nouveautés de Windows Server 2008 R2

Windows Server 2008 R2 propose également certaines fonctionnalités intéressantes concernant l'Active Directory. Parmi ces nouveautés, il y a :

- **Corbeille disponible pour les objets de l'annuaire Active Directory** : si vous supprimez un objet de l'AD (compte utilisateur ou autre), celui-ci sera placé dans la corbeille du contrôleur de domaine durant 180 jours. Vous pouvez alors aisément restaurer cet objet ainsi que tous ses attributs via un clic droit de souris comme vous avez l'habitude de le faire pour un simple fichier. Pour que cette option soit effective, le niveau fonctionnel de la forêt doit nécessairement être 2008 R2 (tous les DC doivent donc être sous Windows Server 2008 R2).

- **Comptes de service gérés (Managed Service Accounts)** : un nouveau type de comptes de domaine voit le jour. Il s'agit des comptes de service géré (traduction approximative car à l'heure où ce livre est écrit, la version R2 n'est pas disponible en français). Ces comptes de service ont pour principal avantage de voir leur mot de passe automatiquement régénéré par le service netlogon (un peu comme les comptes ordinateurs). Le mot de passe d'un compte de service est ainsi automatiquement modifié sans interruption de service et sans aucune intervention. Un compte de service géré ne peut être utilisé que pour un serveur (mais pour plusieurs services).

- **Jonction au domaine en mode déconnecté (Offline domain join)** : la commande `djoin` permet de pré-provisionner un compte ordinateur sur un contrôleur de domaine et de créer le blob associé (*Binary Large OBject*). Ce blob pourra alors être déployé sur le poste client (via le registre ou le fichier VHD) permettant ainsi une jonction automatique du poste client au domaine (après redémarrage). Cette jonction sera possible même si l'ordinateur client ne se trouve pas sur le réseau d'entreprise lors de son redémarrage.

- **Centre d'administration Active Directory** : une nouvelle console de gestion de l'Active Directory voit le jour afin de remplacer la console ADUC. Cette console est un shell graphique pour PowerShell. Après avoir choisi vos modifications de façon graphique via cette console, la commande `PowerShell` correspondante s'affiche à l'écran puis s'exécute (un peu comme le fait déjà Exchange 2007).

Maintenant que vous vous êtes familiarisé avec les fonctionnalités propres à Windows 2008, découvrez une présentation approfondie des stratégies de groupe.

© ENI Editions - All rigths reserved

© ENI Editions - All rigths reserved

Les stratégies de groupe

Les stratégies de groupe sont utilisées au sein d'un domaine Active Directory afin de définir des paramètres communs à un ensemble d'ordinateurs.

Microsoft fournit des améliorations très utiles concernant la gestion des stratégies de groupe sous Windows Server 2008. De nombreuses options supplémentaires ont vu le jour avec cette nouvelle version de Windows et paradoxalement la gestion de ces paramètres a été simplifiée, comparée aux versions précédentes de Windows.

1. Détection des liens lents

La détection des liens lents permet de limiter l'application de certaines stratégies de groupe lorsque l'utilisateur se trouve connecté via un réseau bas débit.

Auparavant cette détection se faisait à l'aide du protocole ICMP avec toutes les contraintes qui vont avec. C'est pour cette raison que Microsoft a développé le service Connaissance des emplacements réseau (appelé aussi NLA pour *Network Location Awareness*) pour Windows Vista et Windows Server 2008. Grâce au service NLA, le rafraîchissement en tâche de fond de vos stratégies de groupe sera bien plus fiable car il ne repose plus sur le protocole ICMP mais RPC, connu pour sa fiabilité. Si votre ordinateur tente de rafraîchir ses stratégies de groupe (par défaut, cela se produit toutes les 90 minutes) alors que le contrôleur de domaine n'est pas accessible à ce moment là (si l'utilisateur n'est pas branché au réseau par exemple), le rafraîchissement ne se fera pas au prochain cycle (donc 90 minutes plus tard) mais dès que le contrôleur de domaine sera à nouveau accessible. Le service NLA permet en effet de détecter très rapidement la disponibilité du contrôleur de domaine dans ce cas de figure.

2. Le format ADMX

Un nouveau format de fichier a vu le jour avec Windows Vista et maintenant Windows Server 2008. Il s'agit des fichiers ADMX. Ces fichiers sont utilisés pour afficher les différentes options des stratégies de groupe.

Ils possèdent de nombreux avantages comparés au format de fichiers précédents (les fichiers ADM). Parmi les principaux avantages de ce nouveau format, il faut retenir :

- Le langage utilisé dans les fichiers AMDX est le XML. Ce format est censé devenir à terme un standard d'échanges d'informations entre applications, faciliter l'interopérabilité, etc.

- La centralisation du stockage des fichiers modèles ADMX dans le dossier SYSVOL alors qu'auparavant les fichiers ADM étaient stockés dans chaque stratégie de groupe de chaque contrôleur de domaine. Il suffit donc simplement de copier/coller les fichiers ADMX d'un poste client sous Windows Vista ou Windows Server 2008 (disponibles dans le dossier c:\Windows\PolicyDefinitions) vers le dossier PolicyDefinitions que vous aurez créé au niveau du partage \\<nom_de_domaine>\SYSVOL\wnom_de_domaine>\Policies. Les administrateurs souhaitant éditer une stratégie n'ont ainsi plus besoin de se soucier de savoir s'ils possèdent les bons fichiers modèles de stratégie puisque ces derniers seront automatiquement récupérés depuis le partage réseau.

- L'indépendance du fichier de langue contenant le texte de chacune des options des stratégies de groupe. Un fichier de langue ayant l'extension .ADML est attaché à chaque fichier ADMX. Il est modifiable à l'aide d'un simple éditeur de texte car il est aussi au format XML. Le détail des modifications engendrées sur le système par le choix d'une stratégie n'est pas contenu dans le fichier ADML mais ADMX associé.

Microsoft fournit par défaut 146 fichiers ADMX et autant de fichiers ADML correspondant à la langue du système d'exploitation. Si vous aviez créé vos propres fichiers modèles de stratégies au format ADM, il vous serait possible de convertir ces derniers au format ADMX à l'aide de l'outil **ADMX Migrator** fourni par Microsoft à l'adresse suivante : http://www.microsoft.com/downloads/details.aspx?FamilyId=0F1EEC3D-10C4-4B5F-9625-97C2F731090C. Cet outil permet également de créer vos propres fichiers ADMX.

3. Journaux de logs

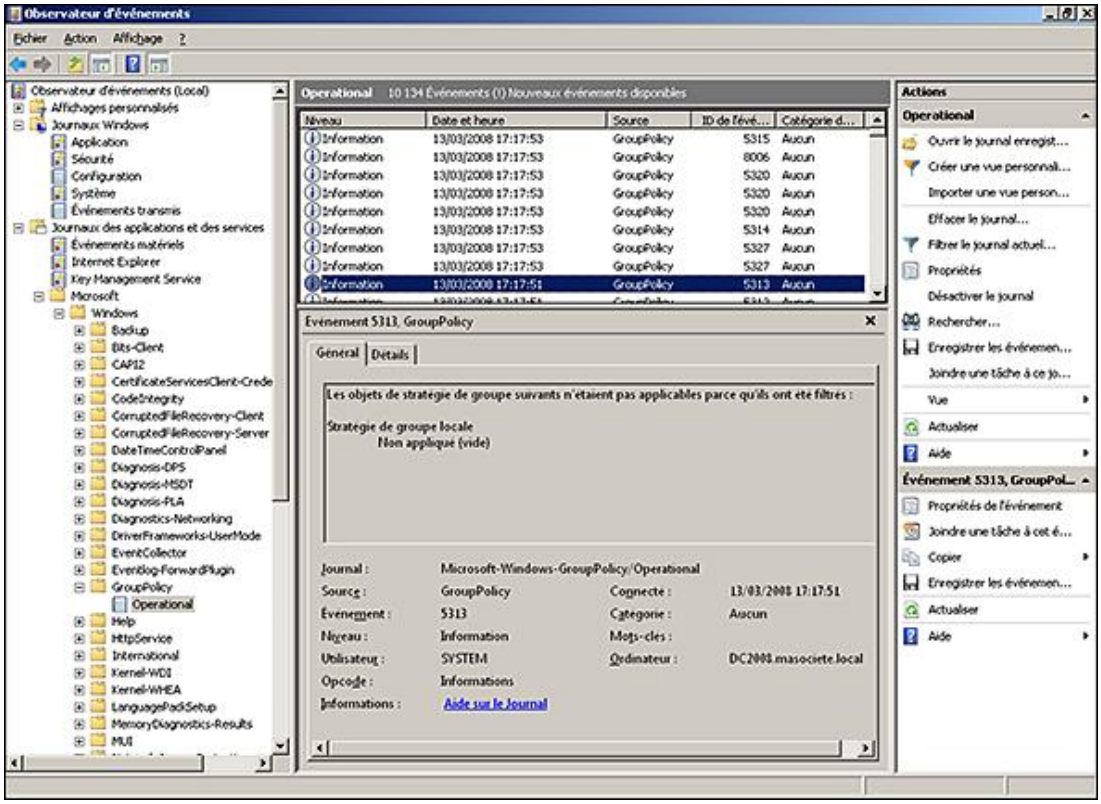
Dans les versions précédentes de Windows, les journaux de logs concernant les stratégies de groupe ont toujours été difficiles à appréhender car le format utilisé était peu parlant pour les administrateurs non-initiés.

Il est désormais possible d'afficher les évènements relatifs aux stratégies de groupe directement depuis le journal des évènements d'un poste sous Windows Vista ou Windows Server 2008.

- Pour cela, cliquez sur le menu **Démarrer** puis **Outils d'administration** et **Observateur d'événements**.

© ENI Editions - All rigths reserved

- Déroulez alors le menu **Journaux des applications et des services - Microsoft - Windows - GroupPolicy - Operational**.



L'outil **Group Policy Log View** vous permettra d'extraire le fichier journal des stratégies de groupe au format TXT ou HTML. Le logiciel est disponible à cette adresse : http://www.microsoft.com/ downloads/details.aspx?FamilyID=BCFB1955-CA1D-4F00-9CFF-6F541BAD4563&displaylang=en

Vous pourrez ainsi beaucoup plus aisément récupérer un grand nombre d'informations concernant le bon fonctionnement ou non des différents paramètres de stratégies de groupe appliqués.

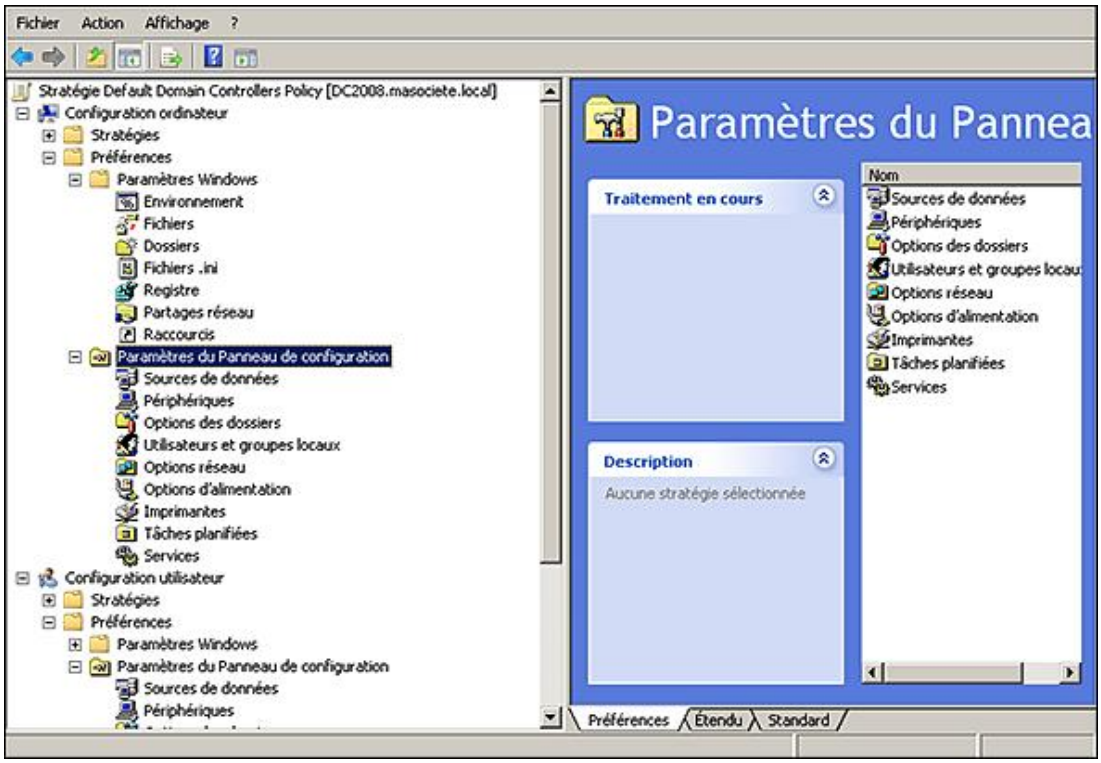
4. Des stratégies de groupe très utiles

Des nouvelles catégories de stratégie de groupe très utiles ont vu le jour dans Windows Server 2008 comme par exemple les *stratégies de groupe de préférences*.

Les *stratégies de groupe de préférences* offrent une alternative aux scripts très souvent utilisés pour la personnalisation de l'environnement utilisateur. Il est en effet possible d'utiliser les stratégies de groupe afin de configurer les lecteurs réseaux, les partages, les utilisateurs et groupes locaux, les options d'alimentation, les imprimantes à installer, les tâches planifiées, etc.

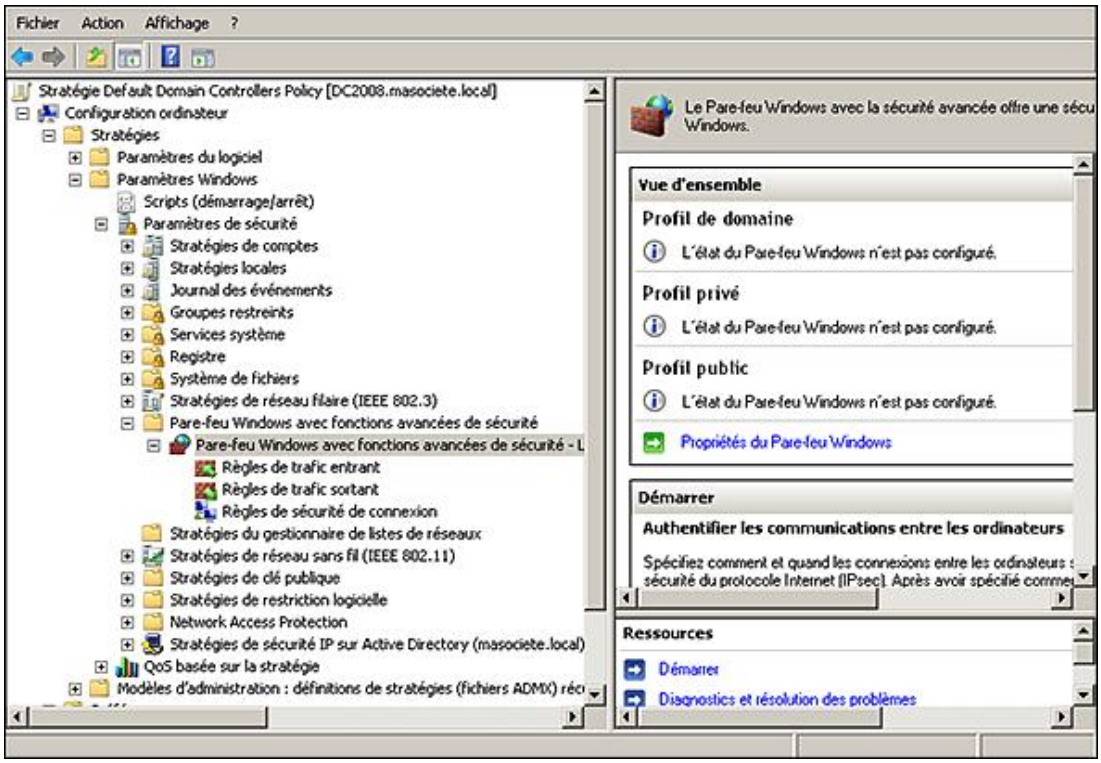
Ces paramètres sont visibles au niveau de **Configuration ordinateur (ou utilisateur) - Préférences - Paramètres du Panneau de configuration**.

© ENI Editions - All rigths reserved



Des options ont également été ajoutées au niveau des paramètres de sécurité comme les stratégies de réseau filaire (IEEE 802.3), les stratégies du gestionnaire de listes de réseaux, le Network Access Protection, etc.

Les paramètres de stratégies du pare-feu et d'IPSec ont été réunis dans une seule console MMC, accessible également depuis n'importe quelle stratégie de groupe. Il est alors possible de définir des règles de trafic entrant, règles de trafic sortant et règles de sécurité de connexion (utilisant le protocole IPSec) pour les clients sous Windows Vista et Windows Server 2008. Ces paramètres seront accessibles depuis **Configuration ordinateur - Paramètres Windows - Pare-feu Windows avec fonctions avancées de sécurité**.


Fichier Action Affichage ?
Stratégie Default Domain Controllers Policy [DC2008.masociete.local]
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 802.3)
Pare-feu Windows avec fonctions avancées de sécurité
Pare-feu Windows avec fonctions avancées de sécurité - L
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de connexion
Stratégies du gestionnaire de listes de réseaux
Stratégies de réseau sans fil (IEEE 802.11)
Stratégies de clé publique
Stratégies de restriction logicielle
Network Access Protection
Stratégies de sécurité IP sur Active Directory (masociete.local)
QoS basée sur la stratégie
Modèles d'administration : définitions de stratégies (fichiers ADMX) réc
Le Pare-feu Windows avec la sécurité avancée offre une sécu
Windows.
Vue d'ensemble
Profil de domaine
L'état du Pare-feu Windows n'est pas configuré.
Profil privé
L'état du Pare-feu Windows n'est pas configuré.
Profil public
L'état du Pare-feu Windows n'est pas configuré.
Propriétés du Pare-feu Windows
Démarrer
Authentifier les communications entre les ordinateurs
Ressources
Démarrer
Diagnostics et résolution des problèmes

Les paramètres de stratégies pour l'IPSec et le pare-feu des anciennes versions de Windows sont toujours accessibles en passant par l'ancien chemin **Configuration ordinateur - Stratégies - Modèles d'administration - Réseau - Connexions réseau - Pare-feu Windows**.

© ENI Editions - All rigths reserved

5. La console Gestion des stratégies de groupe

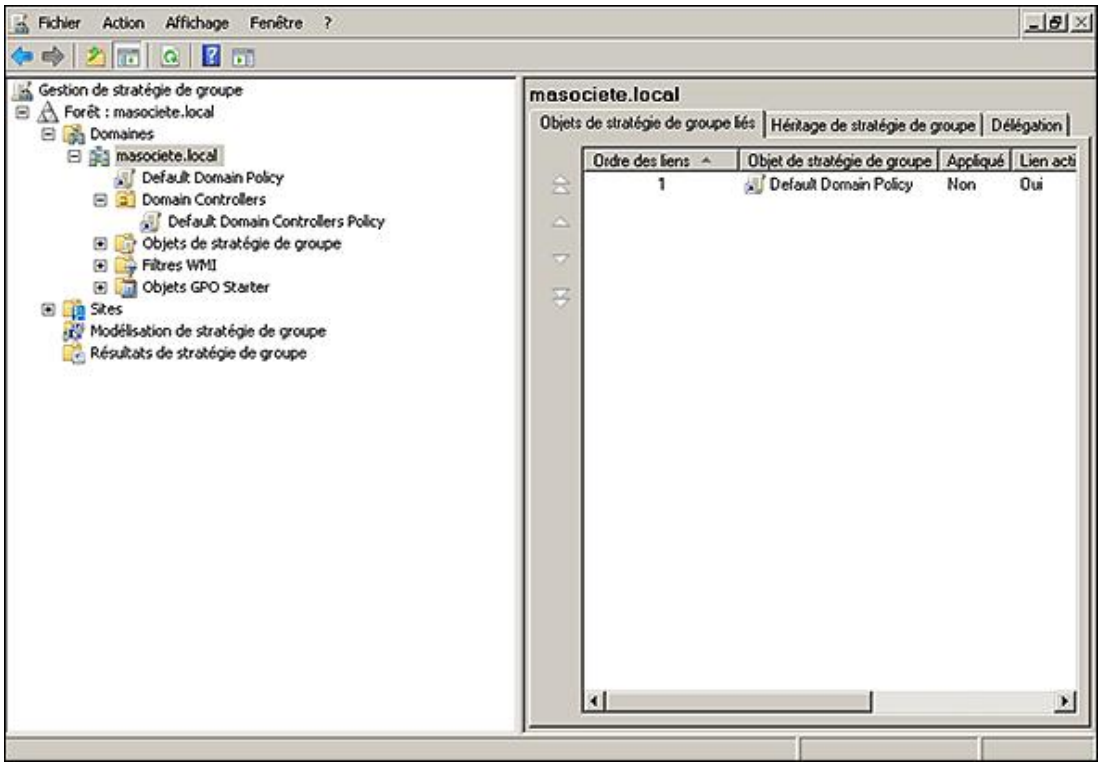
La console Gestion des stratégies de groupe (connue aussi sous le nom de GPMC pour *Group Policy Management Console*) est l'outil indispensable pour gérer vos stratégies de groupe de votre domaine Active Directory.

Si l'ordinateur depuis lequel vous souhaitez éditer les stratégies de groupe ne possède pas la console GPMC, il vous faudra installer cette fonctionnalité depuis le **Gestionnaire de serveur - Ajouter des fonctionnalités** et cochez la case **Gestion des stratégies de groupe**.

L'outil RSAT (pour *Remote Server Administration Tools*) permet de déporter la configuration des stratégies de groupe (et d'une façon générale l'administration des rôles et fonctionnalités de votre serveur) depuis un ordinateur client. Cet outil est téléchargeable sur le site de Microsoft à l'adresse suivante : http://support.microsoft.com/kb/941314

- Afin d'accéder à la console GPMC, cliquez sur le bouton **Démarrer** puis **Outils d'administration** et **Gestion des stratégies de groupe**.

La console vous présentera alors l'organisation du ou des domaines de la forêt de votre choix, leurs OU et sous-OU ainsi que les objets de stratégies de groupe définis.



Cette console vous permet donc de :

- Créer, modifier, supprimer ou lier vos stratégies de groupe au conteneur des sites, domaines ou unités d'organisation de la forêt de votre choix.
- Configurer le filtrage de l'application d'une stratégie (via filtre WMI ou via la sécurité de la stratégie).
- Gérer la délégation.
- Définir des résultats de stratégie de groupe afin de simuler l'application d'une statégie avant sa mise en production.
- Effectuer des sauvegardes/restaurations des stratégies de groupe.
- etc.

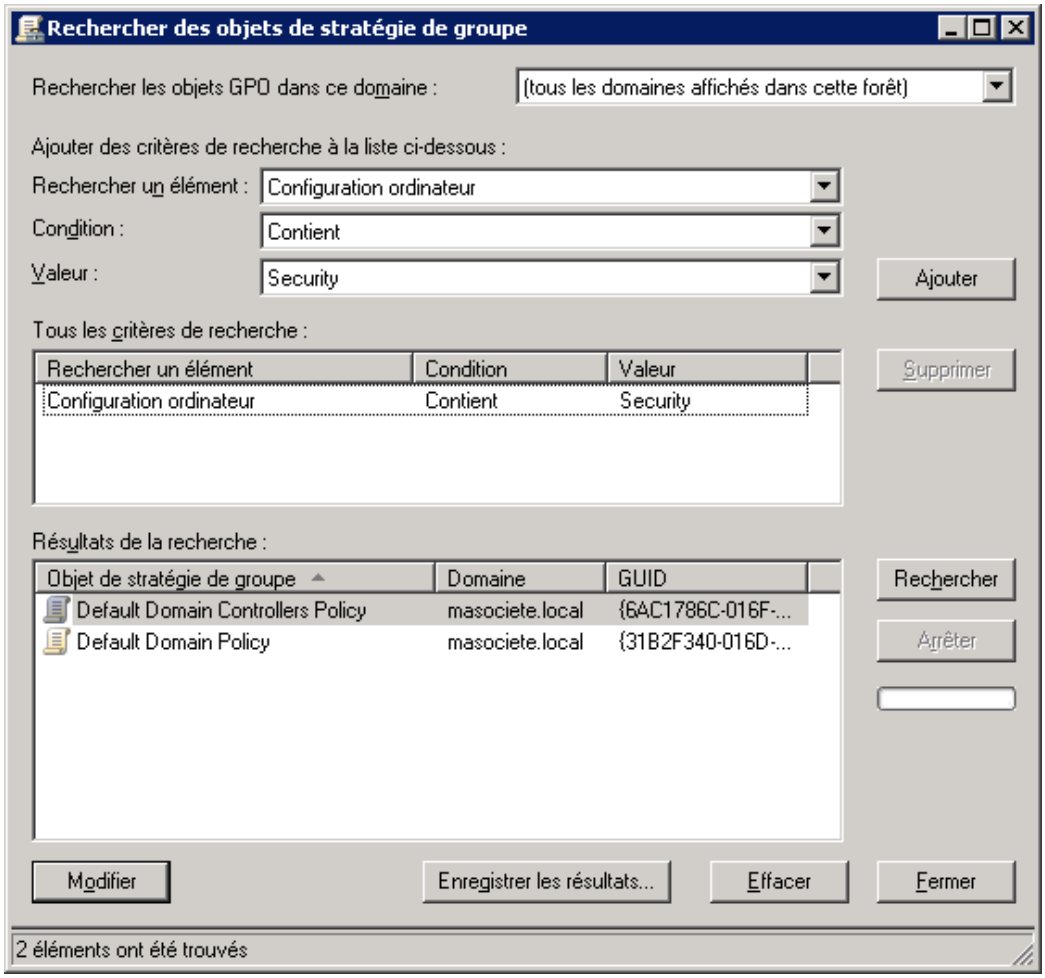
© ENI Editions - All rigths reserved

Parmi ces nombreuses fonctionnalités, il ne faudrait pas oublier deux options qui ont fait leur apparition avec Windows Server 2008. Il s'agit de la possibilité d'effectuer des recherches et de définir des modèles de stratégies.

La fonction **Rechercher** est disponible à deux niveaux dans la console GPMC.

Pour les grosses sociétés gérant un grand nombre d'objets de stratégies de groupe, une fonction **Rechercher** est disponible en faisant un clic avec le bouton droit de la souris sur la forêt ou le domaine de votre choix. Il est alors possible d'afficher les objets de stratégies de groupe répondant à certains critères que vous aurez pris soin de définir.

Il est donc possible de choisir d'afficher les stratégies de groupe pour lesquelles des paramètres de sécurité sont définis.



L'autre fonction **Rechercher** disponible intéressera la plupart d'entre vous. Cette fonction est disponible depuis l'éditeur de gestion des stratégies de groupe. Elle vous permettra de filtrer l'affichage des nombreux paramètres de stratégies se trouvant sous le nœud **Modèles d'administration** en fonction de critères spécifiques.

Vous pouvez ainsi retrouver les paramètres de stratégies répondant à votre besoin sans avoir à naviguer parmi les milliers de paramètres possibles.

Pour utiliser cette option, procédez comme suit :

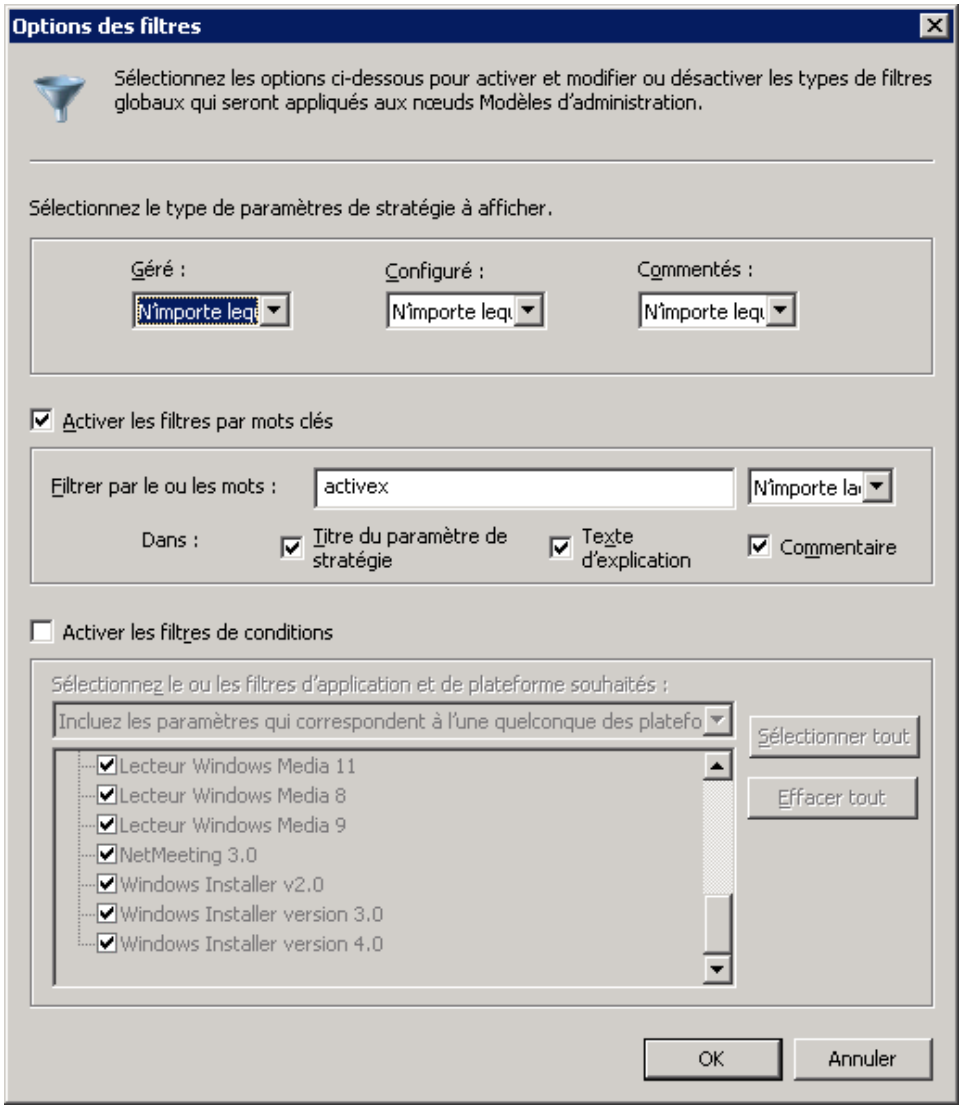
- Depuis votre console GPMC, faites un clic avec le bouton droit de la souris sur l'objet stratégie de groupe que vous souhaitez modifier ; choisissez alors l'option **Modifier** pour accéder à l'éditeur.

- L'éditeur de gestion des stratégies de groupe s'ouvre alors. Naviguez jusqu'au nœud **Modèles d'administration : définitions de stratégies...** via **Configuration ordinateur** (ou **Configuration utilisateur**) - **Stratégies**. Afin d'initier une recherche parmi tous ces paramètres, faites un clic avec le bouton droit de la souris sur ce nœud principal (ou l'un de ses sous-dossiers même si la recherche s'effectuera quoi qu'il arrive sur tous les paramètres de ce nœud) puis choisissez **Options des filtres**.

- Les options des filtres sont divisées en trois catégories vous permettant d'affiner votre recherche. Vous pouvez ainsi choisir d'afficher uniquement les paramètres de stratégie qui sont configurés. Il est également possible d'effectuer un filtrage par mots clés. Enfin, vous pouvez choisir d'afficher les paramètres en définissant des filtres de conditions afin d'afficher en quelques secondes les paramètres applicables à la famille Windows Vista par exemple.

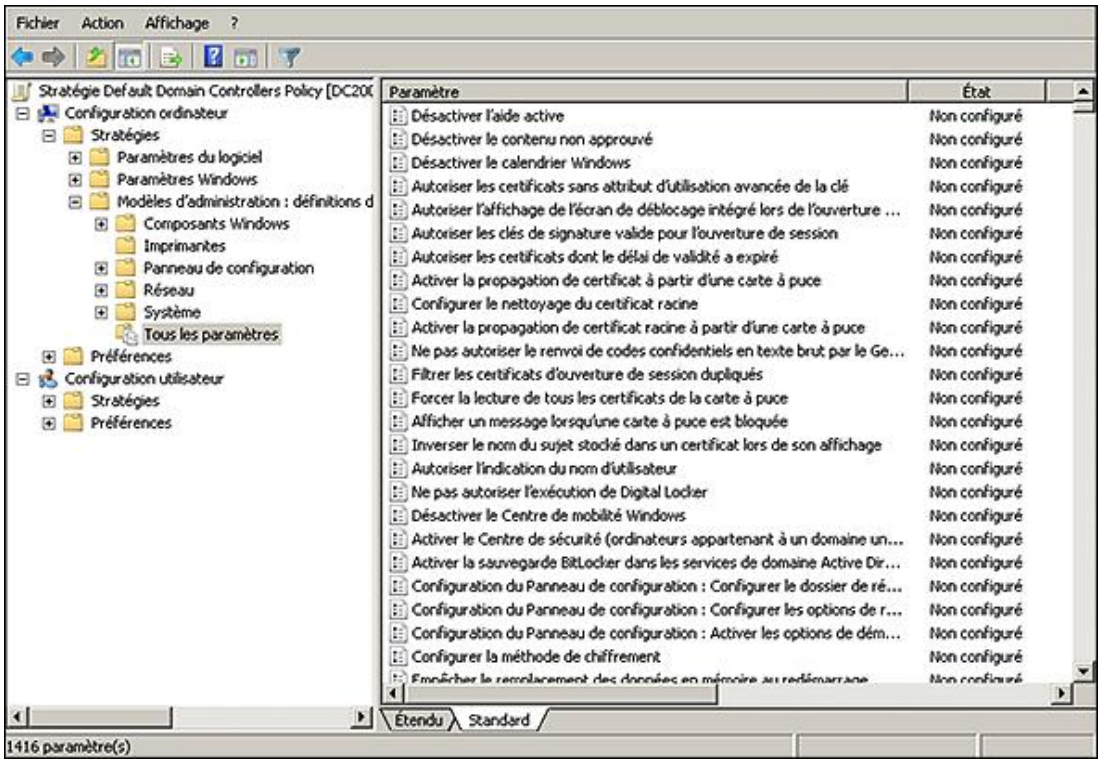
© ENI Editions - All rigths reserved

L'exemple ci-dessous définit un filtre qui affichera tous les paramètres contenant le mot *activeX* dans le titre du paramètre de stratégie, le texte d'explication ou en commentaire (un onglet **commentaire** vous permet en effet d'ajouter le texte de votre choix à la création d'une stratégie de groupe ou à l'activation d'un paramètre). Cliquez alors sur **OK** pour valider le filtre.


Options des filtres
Sélectionnez les options ci-dessous pour activer et modifier ou désactiver les types de filtres globaux qui seront appliqués aux nœuds Modèles d'administration.
Sélectionnez le type de paramètres de stratégie à afficher.
Géré :
N'importe lequ
Configuré :
N'importe lequ
Commentés :
N'importe lequ
Activer les filtres par mots clés
Filtrer par le ou les mots :
activex
N'importe la
Dans :
Titre du paramètre de stratégie
Texte d'explication
Commentaire
Activer les filtres de conditions
Sélectionnez le ou les filtres d'application et de plateforme souhaités :
Incluez les paramètres qui correspondent à l'une quelconque des platefo
Sélectionner tout
Effacer tout
Lecteur Windows Media 11
Lecteur Windows Media 8
Lecteur Windows Media 9
NetMeeting 3.0
Windows Installer v2.0
Windows Installer version 3.0
Windows Installer version 4.0
OK
Annuler

Une fois le filtre validé, l'arborescence de l'éditeur de stratégie se met automatiquement à jour pour n'afficher que les paramètres correspondant au résultat du filtre défini. Ces paramètres sont également regroupés dans le nœud **Tous les paramètres**.

© ENI Editions - All rigths reserved


Fichier Action Affichage ?
Stratégie Default Domain Controllers Policy [DC20
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Modèles d'administration : définitions d
Composants Windows
Imprimantes
Panneau de configuration
Réseau
Système
Tous les paramètres
Préférences
Configuration utilisateur
Stratégies
Préférences
Paramètre
État
Désactiver l'aide active
Désactiver le contenu non approuvé
Désactiver le calendrier Windows
Autoriser les certificats sans attribut d'utilisation avancée de la clé
Autoriser l'affichage de l'écran de déblocage intégré lors de l'ouverture ...
Autoriser les clés de signature valide pour l'ouverture de session
Autoriser les certificats dont le délai de validité a expiré
Activer la propagation de certificat à partir d'une carte à puce
Configurer le nettoyage du certificat racine
Activer la propagation de certificat racine à partir d'une carte à puce
Ne pas autoriser le renvoi de codes confidentiels en texte brut par le Ge...
Filtrer les certificats d'ouverture de session dupliqués
Forcer la lecture de tous les certificats de la carte à puce
Afficher un message lorsqu'une carte à puce est bloquée
Inverser le nom du sujet stocké dans un certificat lors de son affichage
Autoriser l'indication du nom d'utilisateur
Ne pas autoriser l'exécution de Digital Locker
Désactiver le Centre de mobilité Windows
Activer le Centre de sécurité (ordinateurs appartenant à un domaine un...
Activer la sauvegarde BitLocker dans les services de domaine Active Dir...
Configuration du Panneau de configuration : Configurer le dossier de ré...
Configuration du Panneau de configuration : Configurer les options de r...
Configuration du Panneau de configuration : Activer les options de dém...
Configurer la méthode de chiffrement
Étendu
Standard
1416 paramètre(s)

- Pour désactiver le filtre et retrouver un affichage complet, faites un clic avec le bouton droit de la souris sur un des dossiers de **Modèles d'administrations : définitions de stratégies** et enlevez la coche au niveau de **Filtre activé**.

Le filtrage est pour le moment limité aux paramètres définis dans les Modèles d'administration. Si vous souhaitez une liste plus complète (mais non exhaustive) des paramètres regroupant également les paramètres de sécurité, etc, récupérez le fichier Group Policy Settings Reference for Windows Server 2008 and Windows Vista SP1au format XLS ou XLSX : http://www.microsoft.com/downloads/ details.aspx?FamilyID=2043b94e-66cd-4b91-9e0f-68363245c495&DisplayLang=en (disponible en anglais uniquement).

---

6. Les objets GPO Starter

Si vous êtes un peu observateur, vous avez sans doute remarqué en éditant vos stratégies à l'aide de la console GPMC depuis un Windows Server 2008 ou Windows Vista SP1, qu'un nouveau paramètre avait fait son apparition. Il s'agit du conteneur **Objets GPO Starter**.

Cette option consiste à créer des modèles de stratégies de groupe se référant aux paramètres disponibles sous le nœud **Modèles d'administration** uniquement (coté Utilisateurs et Ordinateurs). Il est ainsi très facile de créer plusieurs objets de stratégies de groupe qui se baseront sur un ensemble de paramètres communs devant être définis dans vos stratégies de groupe.

Il est également possible d'exporter ces modèles de GPO dans un fichier CABinet (.CAB) pour alors l'importer dans un environnement totalement différent comme par exemple votre environnement de préproduction.

Lors de la première activation des Objets GPO Starter, un dossier nommé StarterGPOs est créé dans le dossier SYSVOL du contrôleur de domaine. Un nouveau sous-dossier sera créé avec un GUID associé pour chaque nouvel objet GPO Starter.

Afin de planifier une sauvegarde de l'ensemble de vos stratégies, n'oubliez pas de choisir l'option **Sauvegarder tout** disponible depuis le conteneur Objets de Stratégie de Groupe **et** depuis le conteneur Objets GPO Starter.

© ENI Editions - All rigths reserved

Les autres composants Active Directory

Quatre autres principales fonctionnalités en rapport avec l'Active Directory sont disponibles sous Windows Server 2008.

Il s'agit de AD LDS, AD FS, AD RMS et AD CS.

1. Active Directory Lightweight Directory Services (ou AD LDS)

Le rôle AD LDS disponible sous Windows Server 2008 est le nouveau nom de l'ADAM qui avait fait son apparition avec Windows Server 2003 R2.

Il s'agit d'une version épurée de l'Active Directory Domain Services (AD DS) qui repose sur les mêmes fondamentaux (à savoir une réplication multimaîtres, un annuaire divisé en partitions, etc.) mais qui ne stocke aucun composants de sécurité de Windows (comme les comptes utilisateurs et ordinateurs du domaine), les stratégies de groupe, etc.

Le rôle AD LDS permet ainsi de répertorier des informations nécessaires aux applications dans un annuaire centralisé plutôt qu'individuellement dans chaque application. Les avantages de ne pas nécessairement intégrer les applications dans l'AD DS sont divers.

- Une application nécessitant la mise à jour du schéma pourra se faire sur l'AD LDS plutôt que sur l'AD DS, ce qui évitera des risques inutiles de corruption du schéma.
- Une application accessible sur un extranet ou par VPN n'exposera pas l'ensemble du domaine AD DS si elle a pour annuaire de référence un annuaire AD LDS.

À noter qu'il est possible d'avoir plusieurs instances AD LDS sur un même serveur, de même qu'il est possible d'avoir le rôle AD LDS installé sur un Windows Server 2008 possédant le rôle de AD DS. Le seul pré-requis sera que les ports d'écoute des différentes instances devront être différents.

2. Active Directory Federation Services (ou AD FS)

Le composant Active Directory Federation Services permet de mettre en place une solution d'accès sécurisée entre différentes plates-formes Windows ou non-Windows lors d'accès à des applications Web (sur un extranet par exemple).

L'utilité typique de la mise en place d'un AD FS au sein de votre société est de permettre à un client ayant récemment signé un contrat et se connectant depuis un autre réseau (cas d'un B2C), une société partenaire (cas d'un B2B) ou une fédération interentreprises (multiforêts) d'accéder aux ressources de votre réseau d'une façon simple et sans avoir à s'authentifier sur votre base de comptes utilisateurs.

Une relation d'approbation est en effet créée entre le réseau partenaire et le vôtre afin de projeter l'identité des utilisateurs et leurs droits d'accès depuis leur réseau vers les partenaires approuvés. L'utilisateur n'aura ainsi pas à entrer à nouveau ses identifiants (principe de l'authentification unique appelée aussi SSO pour *Single Sign On*).

Il faut savoir également que cette solution est limitée uniquement aux accès via des applications Web (en HTTPS) mais ces dernières étant de plus en plus puissantes, vos possibilités sont très larges. C'est le cas par exemple avec l'intégration de Sharepoint Server 2007 ou de AD RMS que nous présenterons un peu plus tard.

Afin de pouvoir mettre en œuvre l'AD FS, un certain nombre de fonctionnalités et de services devront avoir été mis en place au préalable.

- Le Rôle AD DS ou AD LDS devra être installé sur au moins un des réseaux impliqués.
- Serveur de fédération de comptes/ressources.
- Serveur Web ADFS.
- Client.

Vous trouverez davantage d'informations sur le concept d'AD FS à cette adresse : http://technet.microsoft.com/fr-fr/library/bb821278.aspx

© ENI Editions - All rigths reserved

3. Active Directory Rights Management Services (ou AD RMS)

AD RMS (*Active Directory Right Management*) est un rôle permettant de limiter la diffusion et protéger des fichiers, courriers électroniques ou sites Web de votre société.

AD RMS fonctionne avec des applications compatibles RMS comme le système Microsoft Office 2003 Professionnel, Microsoft Office 2007, Internet Explorer 7.0, etc.

Le principe d'utilisation des fonctionnalités de l'AD RMS repose sur le principe qu'une licence de publication est délivrée à un fichier. L'utilisateur indique alors un ensemble de droits et de conditions spécifiques pour ce document. Ces propriétés le suivront alors afin de le protéger au cours de son cycle de diffusion. Vous serez ainsi capable de contrôler les actions possibles sur un fichier ou son contenu, de définir une durée de validité (pour un devis par exemple), etc.

Ainsi, lorsque le fichier diffusé est ouvert pour la première fois par une application compatible AD RMS, cette dernière contacte le serveur AD RMS ayant émis la licence de publication associée au fichier afin de demander l'autorisation d'accéder à son contenu.

Le serveur AD RMS vérifie alors si l'utilisateur est bien autorisé à visualiser le fichier et si tel est le cas, il envoie une licence d'utilisation au demandeur afin de lui permettre d'accéder au contenu du document. L'utilisateur peut alors ouvrir le fichier à l'aide de l'application compatible RMS.

4. Active Directory Certificate Services (ou AD CS)

Afin d'être complet, il est important d'évoquer le seul rôle que nous n'avons pas encore vu et qui est intimement lié à l'Active Directory. Il s'agit du service de certificats Active Directory (connu aussi sous le nom Active Directory Certification Server ou AD CS).

Il vous permettra d'installer une autorité de certification sur votre réseau d'entreprise afin de pouvoir délivrer des certificats de façon aisée à vos utilisateurs et ordinateurs. Ces derniers pourront ainsi accéder à des sites Web via le protocole SSL sans nécessiter l'achat de certificats (souvent coûteux) auprès d'une autorité de certification publique.

L'avantage certain d'avoir une autorité de certification d'entreprise basée sur Windows Server 2008 est le fait que le processus d'inscription et de renouvellement des certificats est grandement facilité de part l'intégration de cette autorité dans l'Active Directory.

Il existe deux types d'autorité de certifications.

- **Autorité de certification d'entreprise** : nécessite que le serveur possédant le rôle AD CS soit intégré dans l'Active Directory et permet ainsi de profiter de nombreuses fonctionnalités supplémentaires et d'être administrée via les stratégies de groupe.

- **Autorité de certification autonome** : qui peut être installée aussi bien sur un serveur membre ou non mais qui ne profitera pas de fonctionnalités supplémentaires.

La mise en place de cette solution dépassant le cadre de ce livre, voici néanmoins quelques-unes des principales fonctionnalités désormais disponibles sous Windows Server 2008 concernant ce rôle.

- L'inscription des certificats en passant par votre navigateur a été améliorée car elle repose sur un nouveau contrôle nommé CertEnroll.dll.

- Prise en charge du protocole NDES (*Network Device Enrollment Service*) afin de permettre aux périphériques réseaux (routeurs, commutateurs, etc.) d'obtenir des certificats X.509.

- Prise en charge du protocole OSCP (*Online Certificate Status Protocol*) afin d'améliorer la gestion des révocations des certificats.

- Le modèle de certificat en version 3 disponible dans les autorités de certificats d'entreprise prend désormais en charge la cryptographie nouvelle génération (CNG Suite-B).

- Une nouvelle console MMC nommée **PKIView** est désormais disponible afin d'administrer plus efficacement les certificats tout au long de leur cycle de vie.

Vous venez de découvrir au travers de ce chapitre l'ensemble des solutions d'identité et d'accès proposées par Windows Server 2008. Vous pouvez ainsi aborder au mieux les besoins en termes d'accès à des ressources aussi bien pour mettre en place une solution SSO (*Single Sign On* ou "identification unique") que pour contrôler la diffusion de fichiers de votre entreprise.

© ENI Editions - All rigths reserved

© ENI Editions - All rigths reserved

Introduction

Ce chapitre aborde l'architecture distribuée (DFS) par la présentation de l'installation, la configuration des racines, des liaisons, de la réplication DFS-R et des outils utilisables pour réaliser cela.

© ENI Editions - All rigths reserved

La description de DFS

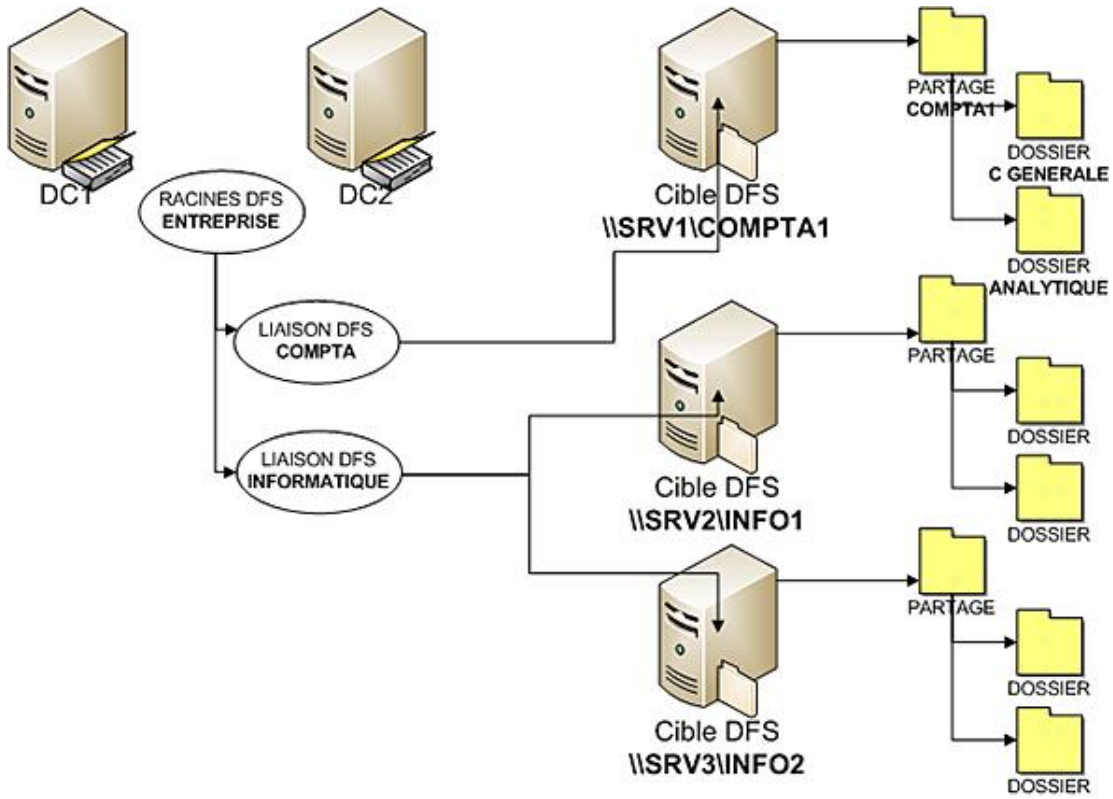
L'acronyme **DFS** signifie *Distributed File Systems*.

C'est un système de fichiers unique, logique, hiérarchisé, qui structure les fichiers partagés sur différents ordinateurs du réseau, sous la forme d'une arborescence logique de ressources système. Le premier objectif de DFS est de référencer tous les partages que l'on veut rendre accessibles de manière uniforme et de centraliser tous les espaces disponibles sur les différents partages.

Ceci permet d'obtenir une vue uniforme et permanente des données qui ne seront plus liées aux serveurs physiques sur lesquels elles se trouvent. Outre l'économie d'unités réseaux, une seule lettre connectée permet d'atteindre tous les partages, les logiciels peuvent être configurés une fois pour toutes sur des chemins précis qui ne bougeront plus même si les données sont déplacées entre deux machines, notamment en cas d'évolution de la volumétrie nécessaire.

Une autre possibilité très intéressante consiste à pouvoir répliquer les données d'un même dossier sur plusieurs liens réseaux, c'est-à-dire sur plusieurs partages. Cette tolérance de pannes apporte une fonctionnalité assez proche d'un cluster de fichiers. Mais, il faut néanmoins bien étudier son mode opératoire pour éviter toute surprise.

Voici comment DFS organise les ressources résidantes sur différents composants d'un réseau :



L'arborescence DFS constituant un point unique de référence, quel que soit l'emplacement des ressources, les utilisateurs peuvent accéder aisément aux ressources du réseau. Sur le réseau, les unités DFS sont vues comme des partages réseaux classiques et sont donc gérées par la fonction « redirecteur de fichiers» des clients réseaux classiques.

Un utilisateur naviguant dans un dossier partagé DFS n'a pas à connaître le nom ni la localisation du serveur sur lequel se trouve une ressource particulière. L'accès aux ressources réseau s'en trouve donc simplifié. Après s'être connecté à une racine DFS, il peut parcourir la structure et accéder à toutes les ressources situées sous cette racine. Un partage DFS utilise une structure d'arborescence contenant une racine et des liaisons DFS.

Pour démarrer l'utilisation de DFS, il faut tout d'abord créer une racine DFS. Depuis Windows 2003, il est possible de créer plusieurs racines. Chaque racine peut comporter plusieurs liaisons, chacune d'elle pointant vers un dossier partagé sur le réseau. Les liaisons DFS de la racine DFS représentent des dossiers partagés pouvant être physiquement localisés sur différents services de fichiers. Les avantages liés à DFS sont décrits ci-après :

Pour résumer, voici tous les avantages de cette solution :

- L'administration du réseau est simplifiée. En cas de défaillance d'un serveur, la liaison DFS peut être déplacée sur un autre serveur, en modifiant le dossier DFS pour indiquer le nouveau serveur d'hébergement des dossiers partagés. Le chemin reste le même pour les utilisateurs.

© ENI Editions - All rigths reserved

- L’espace de noms permet un accès à toutes les ressources par un nom unique, sans avoir à mapper de lettre sur chaque ressource.

- DFS est intégré aux clients Windows et ne requiert pas d’agent ou de mémoire supplémentaire.

- Les serveurs de fichiers peuvent être remplacés sans affecter l’espace de noms utilisé par les clients.

- L’équilibrage et la tolérance de panne peuvent être obtenus sur les racines et sur les liaisons à protéger en indiquant plusieurs serveurs et partages sur chaque ressource. Différents cadres d’utilisation sont alors possibles.

- L’espace de noms peut être étendu dynamiquement pour inclure un espace disque complémentaire ou prendre en charge de nouveaux besoins.

- DFS utilise toutes les autorisations existantes. Aucune règle ou autorisation supplémentaire ne sont nécessaires pour les utilisateurs. Les listes de contrôle d’accès (ACL) situées sur des dossiers répliqués sont répliquées de la même manière que les données.

- Afin d’accélérer la recherche et le parcours de l’arborescence DFS, celle-ci est automatiquement mise en cache sur les clients lors de la première utilisation jusqu’à l’arrêt du client ou l’expiration du mot de passe.

© ENI Editions - All rigths reserved

L’installation

Contrairement aux anciennes versions, les modules DFS ne sont plus intégrés et démarrés automatiquement sur les serveurs Windows. La seule exception, mais de taille, se situe sur les contrôleurs de domaine qui utilisent la réplication DFS pour les dossiers de partages SYSVOL.

Le module `FS-DFS` est composé de deux sous-modules :

- `FS-DFS -namespace`
- `FS-DFS -Replication`

L’ensemble des modules peut être installé par script avec la commande suivante :

```
servermanagercmd -install FS-DFS
```

Les deux modules peuvent être utilisés séparément et répondre à des besoins différents. On peut très bien soit répliquer des dossiers, soit publier des espaces, mais l’utilisation idéale **consiste à utiliser les deux fonctions**.

1. Le module d’espace de noms

Comme dans Windows 2003, plusieurs espaces de nommages peuvent être créés. Ces espaces sont publiés dans Active Directory (AD).

L’installation du module d’espace de noms peut se faire par la commande :

```
servermanagercmd -install FS-DFS -namespace
```

2. Le module de réplication

Le module de réplication permet de créer des groupes de réplications de données. Une réplication doit contenir au moins deux partages provenant de deux serveurs différents.

L’installation du module de réplication peut se faire par la commande :

```
servermanagercmd -install FS-DFS-Replication
```

À noter que la réplication par les outils Microsoft n’est pas obligatoire. Il est possible d’utiliser les liaisons DFS pour pointer sur plusieurs partages. Mais, si l’on veut un contenu identique, celui-ci devra être placé de manière « explicite » par des outils ou des scripts adéquats.

3. La console d’administration

Si nécessaire, la console d’administration peut être installée séparément des deux autres modules dans les fonctionnalités.

La console d’administration se trouve dans la partie :

- Outils d’administration de serveur distants
- Outils d’administration des rôles
- Outils de services de fichiers
- Outils du système de fichiers DFS

L’installation peut aussi se faire par script :

```
Servermanagercmd -install RSAT-MGMT-DFS-con
```

© ENI Editions - All rigths reserved

Après lancement de la console, il suffira d'interroger AD pour obtenir la liste des racines DFS existantes.

4. Le cas des contrôleurs de domaine

Sur un contrôleur de domaine, les services d'espace de noms et de réplication sont installés automatiquement, mais AD gère directement ses propres dossiers partagés. Il n'est donc pas possible de voir ou de modifier à ce niveau la réplication utilisée par Active Directory pour répliquer le partage SYSVOL.

5. La cohabitation avec DFS 2003

Si l'on veut répliquer des données avec des racines DFS hébergées par Windows 2003 ou Windows 2000, il faudra installer un module spécifique de réplication basé sur l'ancien système de réplication de fichiers FRS. Ce module de réplication se trouve dans le rôle **services de fichiers** et sera installé par l'ajout du service de rôles **Service de réplication de fichiers**.

L'installation peut aussi se faire par script :

```
Servermanagercmd -install FS-Replication
```

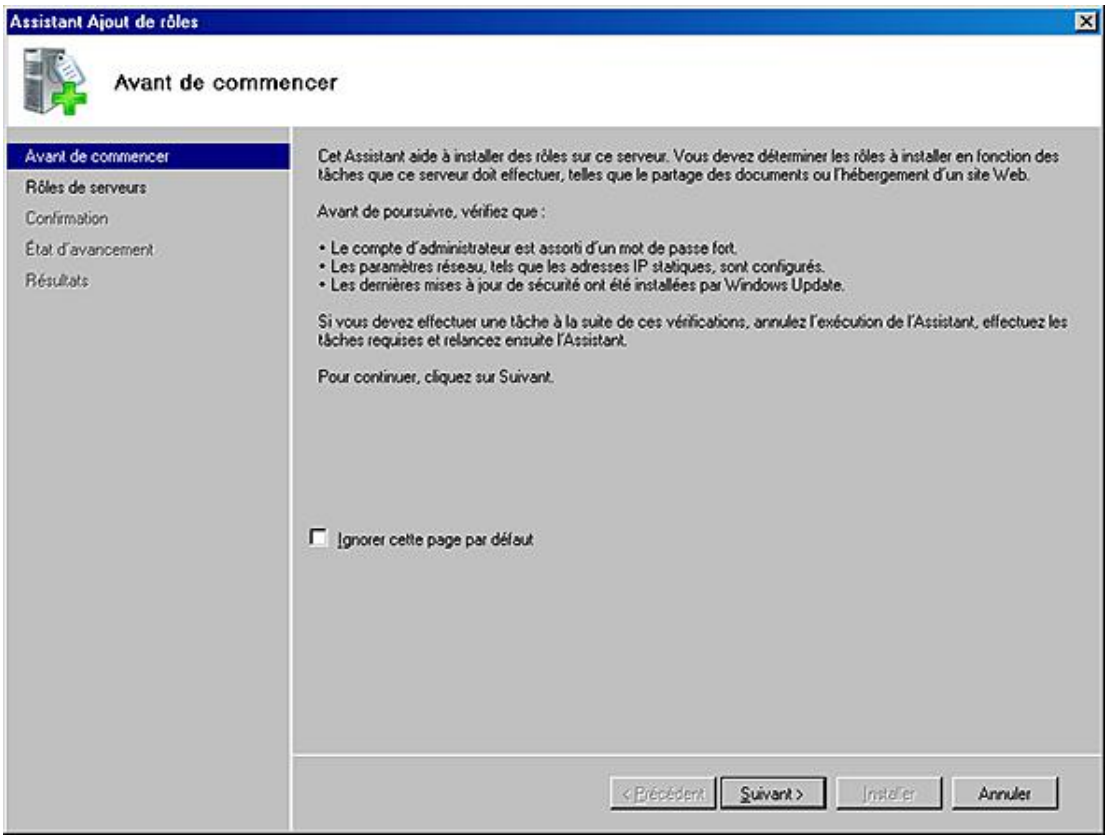
6. La procédure d'installation graphique

L'installation graphique permet d'ajouter tous les composants nécessaires en une seule opération. Celle-ci se fait à partir de l'outil **Gestionnaire de Serveur**, dans la ruche **Rôles**, en cliquant sur **Ajout des rôles**.

Voici les différentes étapes :

- Cliquez sur **Suivant**.

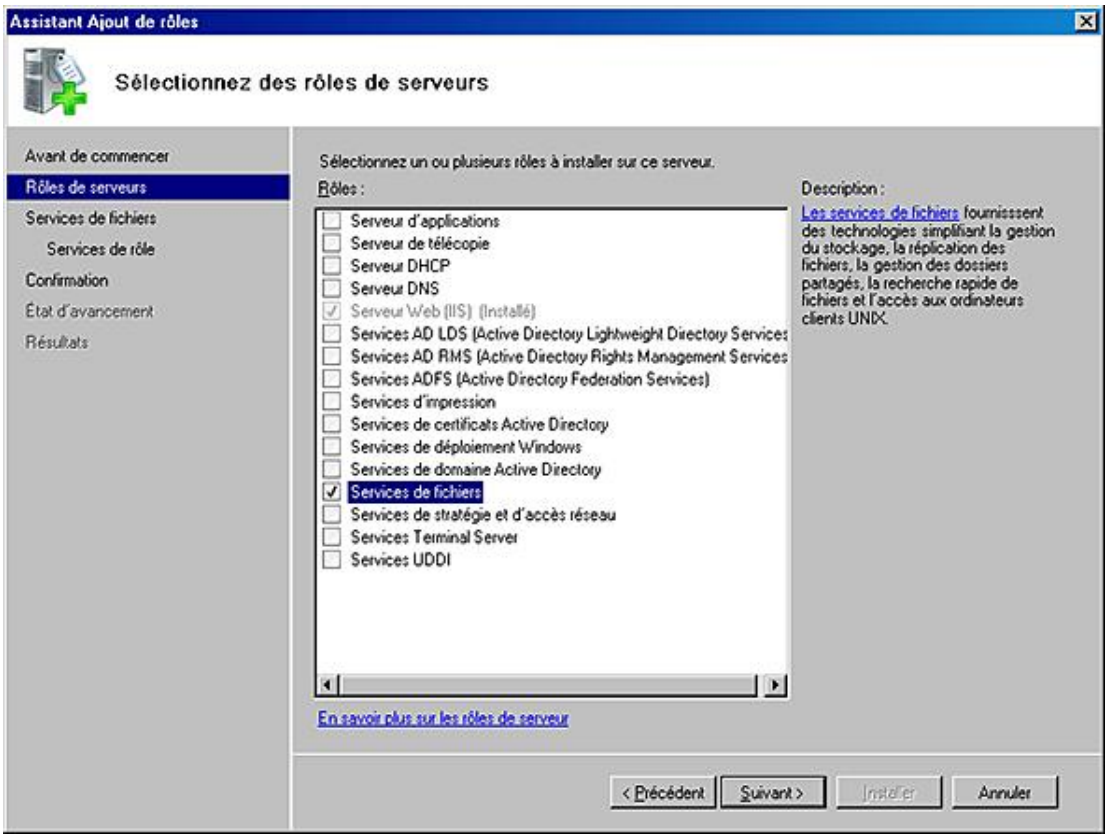
Cette étape peut ensuite être ignorée en cochant la case adéquate.


Assistant Ajout de rôles
Avant de commencer
Avant de commencer
Rôles de serveurs
Confirmation
État d'avancement
Résultats
Cet Assistant aide à installer des rôles sur ce serveur. Vous devez déterminer les rôles à installer en fonction des tâches que ce serveur doit effectuer, telles que le partage des documents ou l'hébergement d'un site Web.
Avant de poursuivre, vérifiez que :
• Le compte d'administrateur est assorti d'un mot de passe fort.
• Les paramètres réseau, tels que les adresses IP statiques, sont configurés.
• Les dernières mises à jour de sécurité ont été installées par Windows Update.
Si vous devez effectuer une tâche à la suite de ces vérifications, annulez l'exécution de l'Assistant, effectuez les tâches requises et relancez ensuite l'Assistant.
Pour continuer, cliquez sur Suivant.
Ignorer cette page par défaut
< Précédent
Suivant >
Installer
Annuler

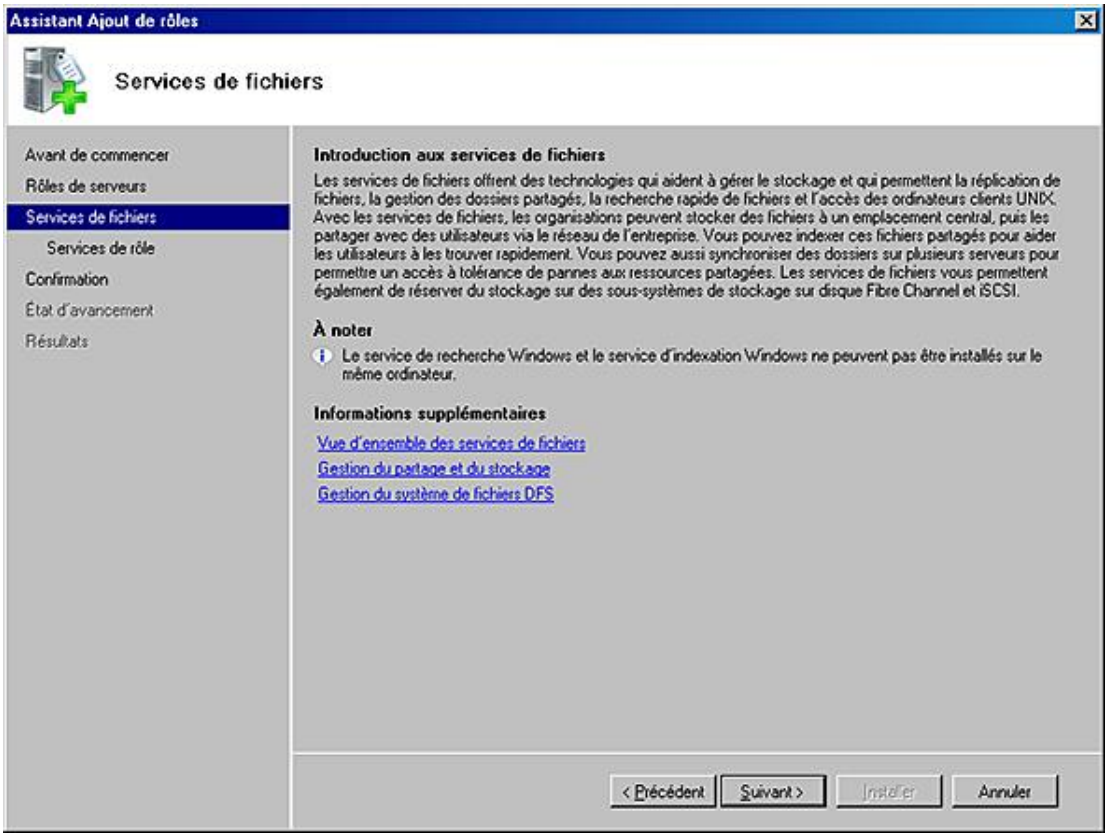
- Sélectionnez le rôle **Services de fichiers**.

© ENI Editions - All rigths reserved

Les cases cochées et grisées indiquent les rôles qui sont déjà présents sur cette machine.


Assistant Ajout de rôles
Sélectionnez des rôles de serveurs
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionnez un ou plusieurs rôles à installer sur ce serveur.
Rôles :
Serveur d'applications
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS) (Installé)
Services AD LDS (Active Directory Lightweight Directory Services
Services AD RMS (Active Directory Rights Management Services
Services ADFS (Active Directory Federation Services)
Services d'impression
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory
Services de fichiers
Services de stratégie et d'accès réseau
Services Terminal Server
Services UDDI
Description :
Les services de fichiers fournissent des technologies simplifiant la gestion du stockage, la réplication des fichiers, la gestion des dossiers partagés, la recherche rapide de fichiers et l'accès aux ordinateurs clients UNIX.
En savoir plus sur les rôles de serveur
< Précédent
Suivant >
Installer
Annuler

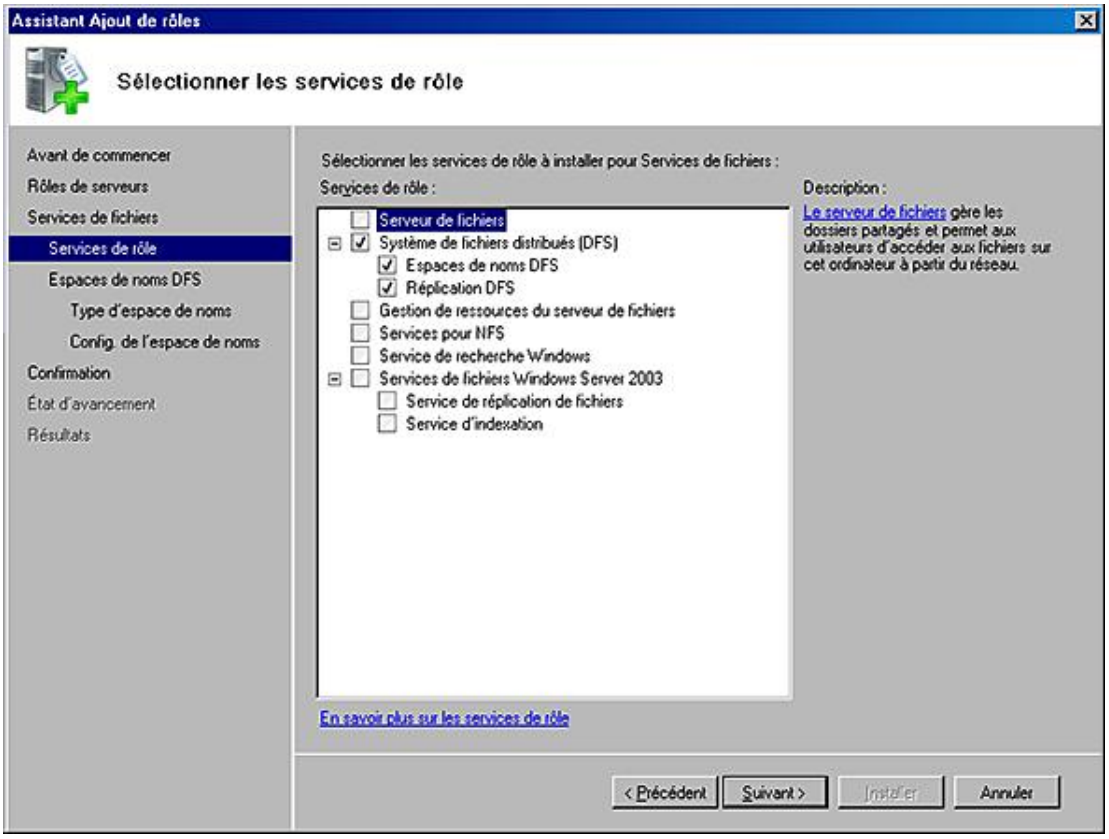
Cette page permet d'obtenir une aide précieuse lors des premières installations.


Assistant Ajout de rôles
Services de fichiers
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Confirmation
État d'avancement
Résultats
Introduction aux services de fichiers
Les services de fichiers offrent des technologies qui aident à gérer le stockage et qui permettent la réplication de fichiers, la gestion des dossiers partagés, la recherche rapide de fichiers et l'accès des ordinateurs clients UNIX. Avec les services de fichiers, les organisations peuvent stocker des fichiers à un emplacement central, puis les partager avec des utilisateurs via le réseau de l'entreprise. Vous pouvez indexer ces fichiers partagés pour aider les utilisateurs à les trouver rapidement. Vous pouvez aussi synchroniser des dossiers sur plusieurs serveurs pour permettre un accès à tolérance de pannes aux ressources partagées. Les services de fichiers vous permettent également de réserver du stockage sur des sous-systèmes de stockage sur disque Fibre Channel et iSCSI.
À noter
Le service de recherche Windows et le service d'indexation Windows ne peuvent pas être installés sur le même ordinateur.
Informations supplémentaires
Vue d'ensemble des services de fichiers
Gestion du partage et du stockage
Gestion du système de fichiers DFS
< Précédent
Suivant >
Installer
Annuler

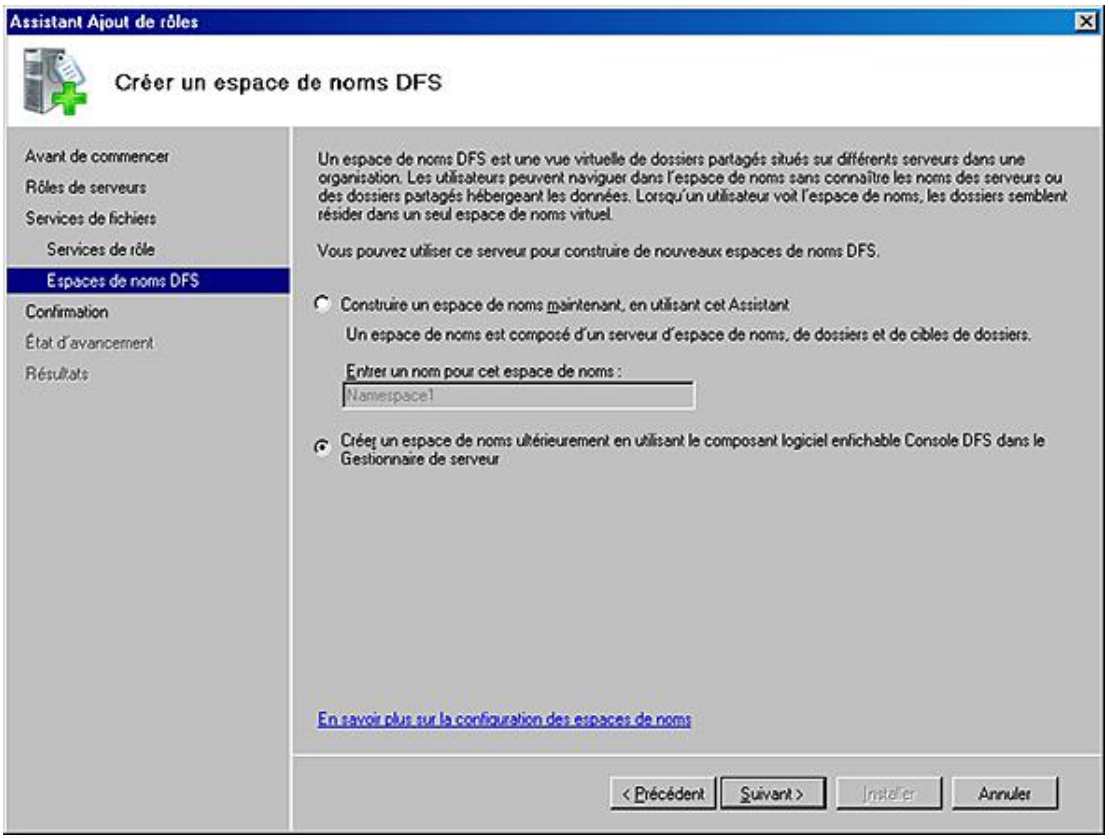
- Il suffit ensuite de sélectionner parmi les **Services de rôle** les composants souhaités.

© ENI Editions - All rigths reserved

À noter que le module **Service de réplication de fichiers** dans **Services de fichiers Windows Server 2003** devra être sélectionné s'il est nécessaire de répliquer vers des cibles DFS Windows 2003 ou 2000.

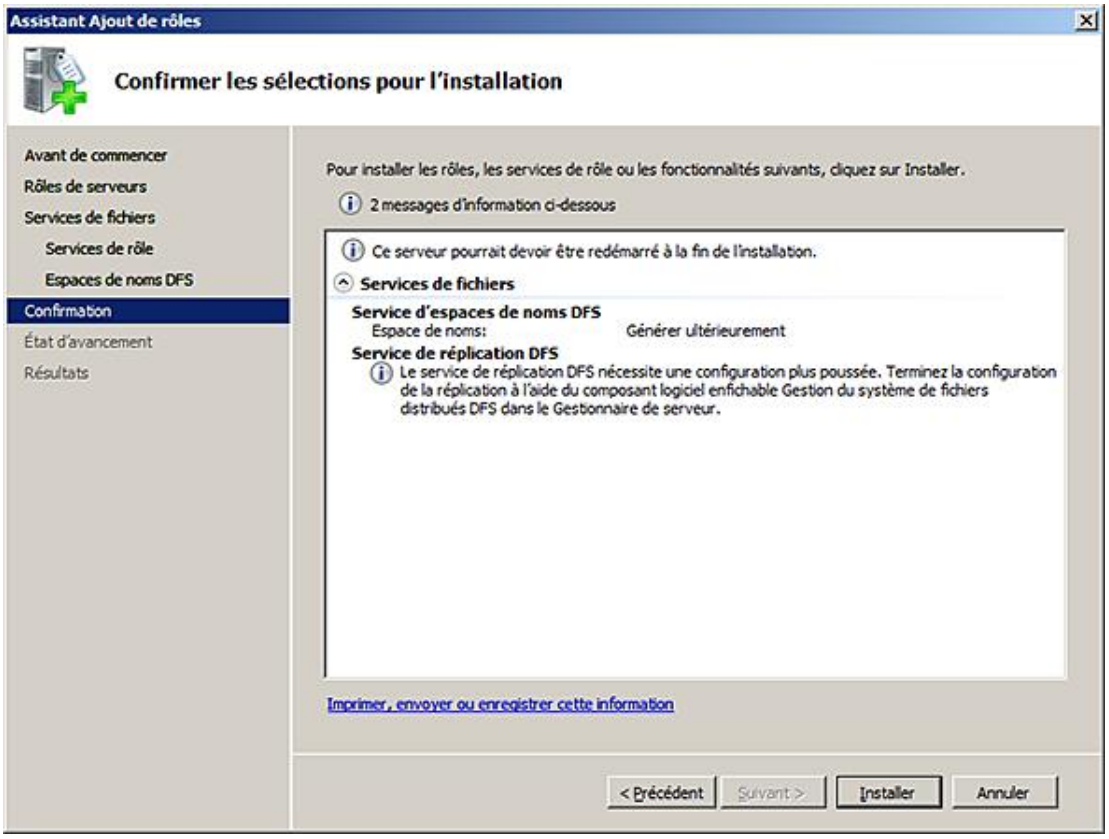

Assistant Ajout de rôles
Sélectionner les services de rôle
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Espaces de noms DFS
Type d'espace de noms
Config. de l'espace de noms
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Services de fichiers :
Services de rôle :
Serveur de fichiers
Système de fichiers distribués (DFS)
Espaces de noms DFS
Réplication DFS
Gestion de ressources du serveur de fichiers
Services pour NFS
Service de recherche Windows
Services de fichiers Windows Server 2003
Service de réplication de fichiers
Service d'indexation
Description :
Le serveur de fichiers gère les dossiers partagés et permet aux utilisateurs d'accéder aux fichiers sur cet ordinateur à partir du réseau.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler

Il est possible de créer immédiatement un premier espace de noms. Mais, vous retrouverez cette opération plus tard.

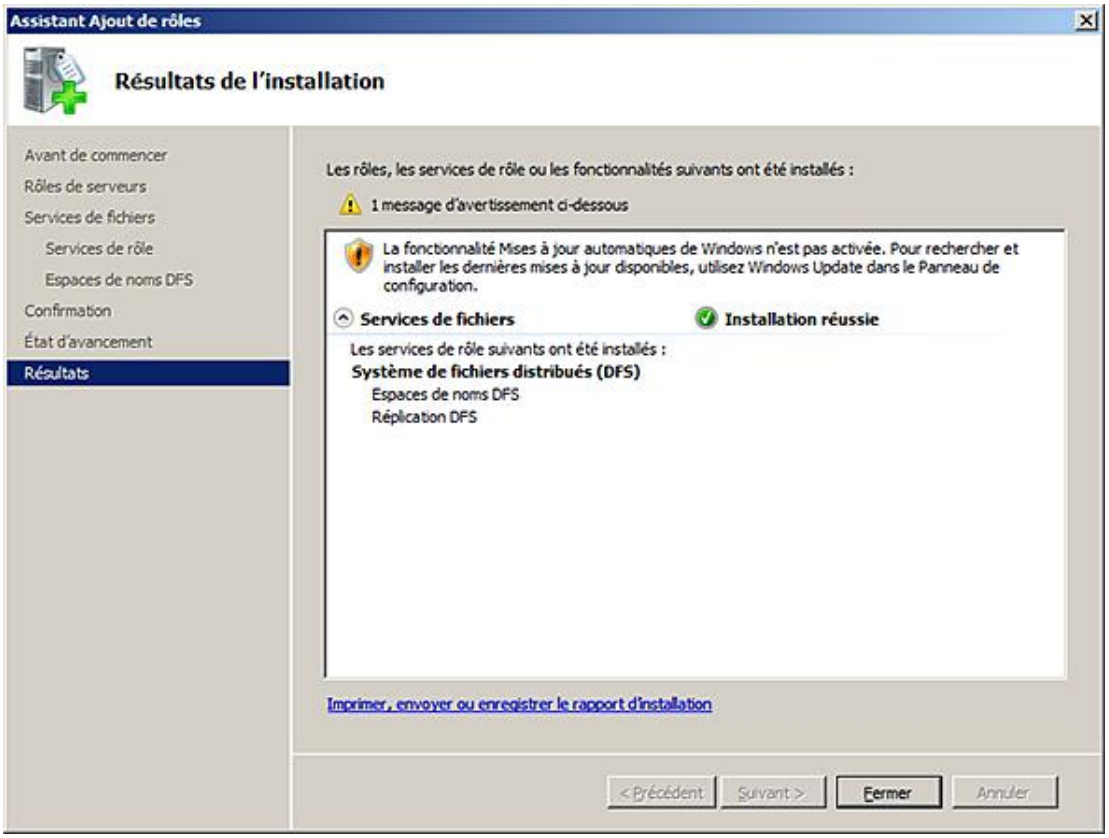

Assistant Ajout de rôles
Créer un espace de noms DFS
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Espaces de noms DFS
Confirmation
État d'avancement
Résultats
Un espace de noms DFS est une vue virtuelle de dossiers partagés situés sur différents serveurs dans une organisation. Les utilisateurs peuvent naviguer dans l'espace de noms sans connaître les noms des serveurs ou des dossiers partagés hébergeant les données. Lorsqu'un utilisateur voit l'espace de noms, les dossiers semblent résider dans un seul espace de noms virtuel.
Vous pouvez utiliser ce serveur pour construire de nouveaux espaces de noms DFS.
Construire un espace de noms maintenant, en utilisant cet Assistant
Un espace de noms est composé d'un serveur d'espace de noms, de dossiers et de cibles de dossiers.
Entrer un nom pour cet espace de noms :
Namespace1
Créer un espace de noms ultérieurement en utilisant le composant logiciel enfichable Console DFS dans le Gestionnaire de serveur
En savoir plus sur la configuration des espaces de noms
< Précédent
Suivant >
Installer
Annuler

- Cliquez sur **Installer**.

© ENI Editions - All rigths reserved

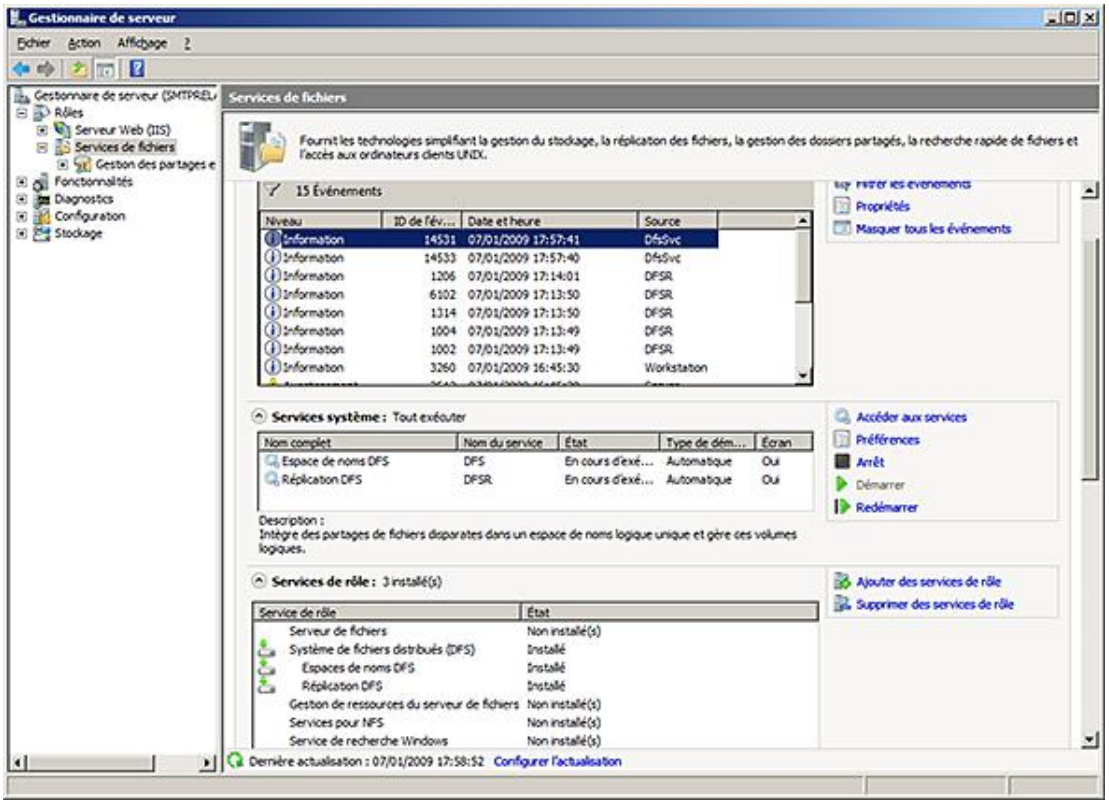

Assistant Ajout de rôles
Confirmer les sélections pour l'installation
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Espaces de noms DFS
Confirmation
État d'avancement
Résultats
Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer.
2 messages d'information ci-dessous
Ce serveur pourrait devoir être redémarré à la fin de l'installation.
Services de fichiers
Service d'espaces de noms DFS
Espace de noms: Générer ultérieurement
Service de réplication DFS
Le service de réplication DFS nécessite une configuration plus poussée. Terminez la configuration de la réplication à l'aide du composant logiciel enfichable Gestion du système de fichiers distribués DFS dans le Gestionnaire de serveur.
Imprimer, envoyer ou enregistrer cette information
< Précédent
Suivant >
Installer
Annuler

- Cliquez sur **Fermer**.


Assistant Ajout de rôles
Résultats de l'installation
Avant de commencer
Rôles de serveurs
Services de fichiers
Services de rôle
Espaces de noms DFS
Confirmation
État d'avancement
Résultats
Les rôles, les services de rôle ou les fonctionnalités suivants ont été installés :
1 message d'avertissement ci-dessous
La fonctionnalité Mises à jour automatiques de Windows n'est pas activée. Pour rechercher et installer les dernières mises à jour disponibles, utilisez Windows Update dans le Panneau de configuration.
Services de fichiers
Installation réussie
Les services de rôle suivants ont été installés :
Système de fichiers distribués (DFS)
Espaces de noms DFS
Réplication DFS
Imprimer, envoyer ou enregistrer le rapport d'installation
< Précédent
Suivant >
Fermer
Annuler

Après installation, les services sont démarrés automatiquement et apparaissent dans les services de rôles.

© ENI Editions - All rigths reserved


Gestionnaire de serveur
Fichier Action Affichage ?
Gestionnaire de serveur (SMTPREL
Rôles
Serveur Web (IIS)
Services de fichiers
Gestion des partages e
Fonctionnalités
Diagnostics
Configuration
Stockage
Services de fichiers
Fournit les technologies simplifiant la gestion du stockage, la réplication des fichiers, la gestion des dossiers partagés, la recherche rapide de fichiers et l'accès aux ordinateurs clients UNIX.
15 Événements
Niveau ID de l'év... Date et heure Source
Information 14531 07/01/2009 17:57:41 Dfssvc
Information 14533 07/01/2009 17:57:40 Dfssvc
Information 1206 07/01/2009 17:14:01 DFSR
Information 6102 07/01/2009 17:13:50 DFSR
Information 1314 07/01/2009 17:13:50 DFSR
Information 1004 07/01/2009 17:13:49 DFSR
Information 1002 07/01/2009 17:13:49 DFSR
Information 3260 07/01/2009 16:45:30 Workstation
Propriétés
Masquer tous les événements
Services système : Tout exécuter
Nom complet Nom du service État Type de dém... Écran
Espace de noms DFS DFS En cours d'exé... Automatique Oui
Réplication DFS DFSR En cours d'exé... Automatique Oui
Accéder aux services
Préférences
Arrêt
Démarrer
Redémarrer
Description :
Intègre des partages de fichiers disparates dans un espace de noms logique unique et gère ces volumes logiques.
Services de rôle : 3 installé(s)
Service de rôle État
Serveur de fichiers Non installé(s)
Système de fichiers distribués (DFS) Installé
Espaces de noms DFS Installé
Réplication DFS Installé
Gestion de ressources du serveur de fichiers Non installé(s)
Services pour NFS Non installé(s)
Service de recherche Windows Non installé(s)
Ajouter des services de rôle
Supprimer des services de rôle
Dernière actualisation : 07/01/2009 17:58:52 Configurer l'actualisation

© ENI Editions - All rigths reserved

La configuration

1. Les différents types de racines distribuées

a. Les racines Autonomes

Les racines autonomes permettent de créer des arborescences qui ne sont liées qu'à un serveur précis. Ces racines ne sont pas sécurisées, c'est-à-dire que la racine DFS ne sera plus ni accessible, ni utilisable si le serveur qui l'héberge ne fonctionne pas correctement. En revanche, les accès directs aux partages restent fonctionnels.

À noter que les dossiers (liens de partages) peuvent quand même être répliqués et synchronisés par un groupe de réplication spécifique.

Par ailleurs, si la racine autonome est configurée sur un cluster de fichiers, la racine DFS profitera de la même tolérance aux pannes que le partage de fichiers. Mais ceci ne sera possible que sur un cluster Windows 2008.

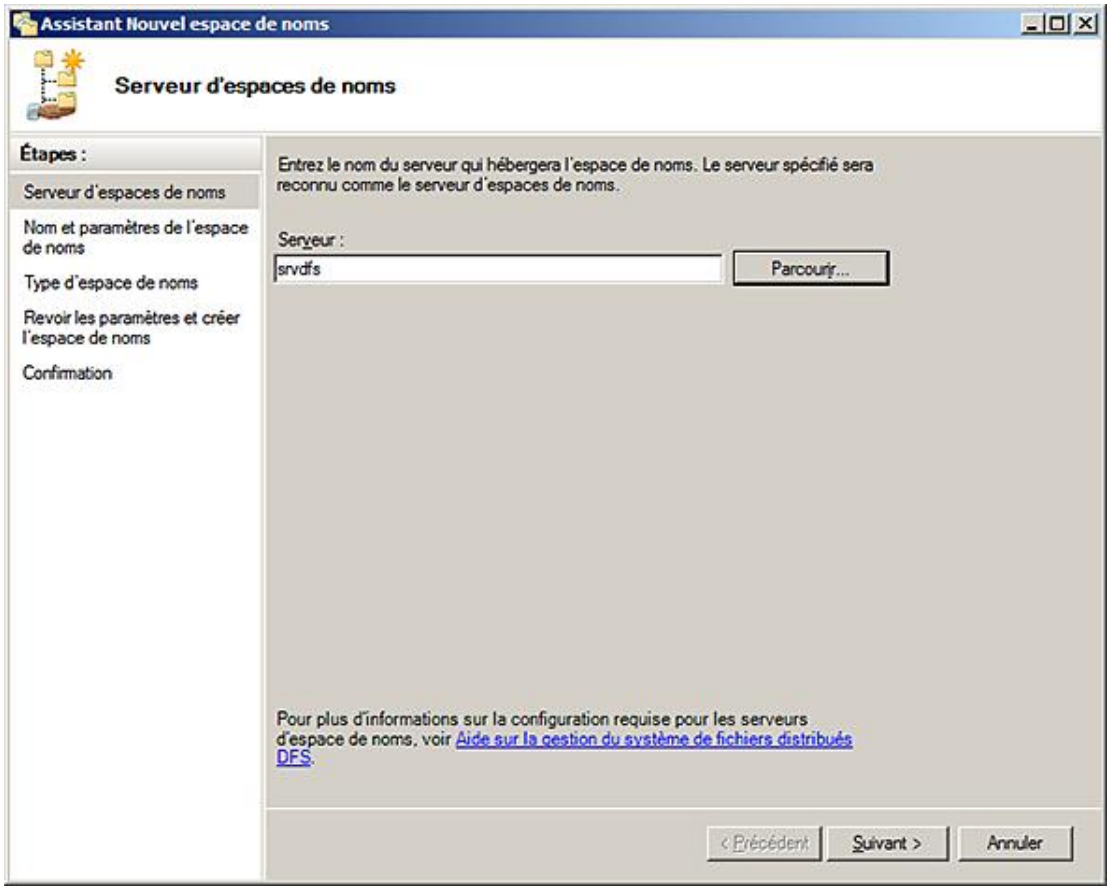
Voici la procédure de création d'une racine autonome.

En utilisant l'assistant de création d'un espace de nommage **Nouvel espace de noms**, ceci peut se créer très rapidement.

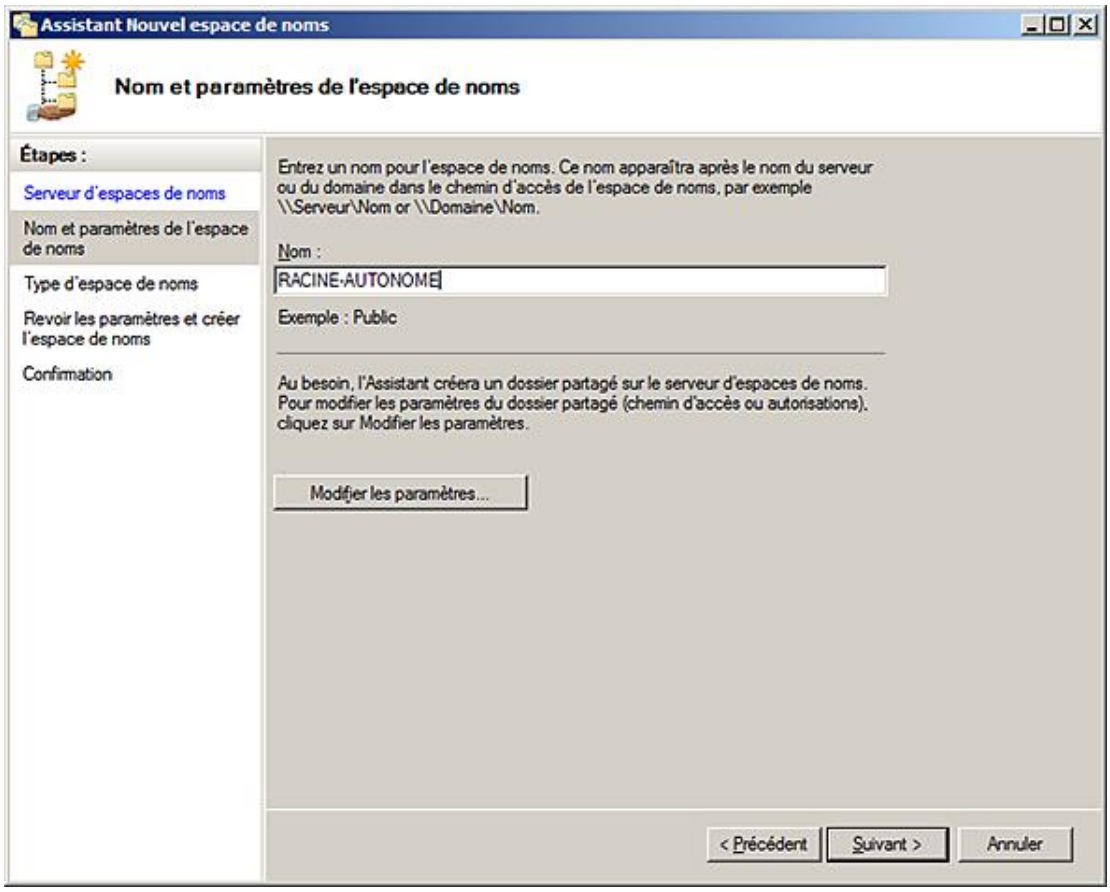
- Utilisez le bouton droit sur **Espaces de noms** pour faire apparaître le menu.

Les serveurs d'espaces de noms n'ont pas vocation à recevoir directement des données. Ils ne contiennent normalement que des dossiers **virtuels** qui eux, pointent sur des données réelles. Ce sont souvent des serveurs contrôleurs de domaine qui sont choisis pour suivre ce type d'information.

© ENI Editions - All rigths reserved

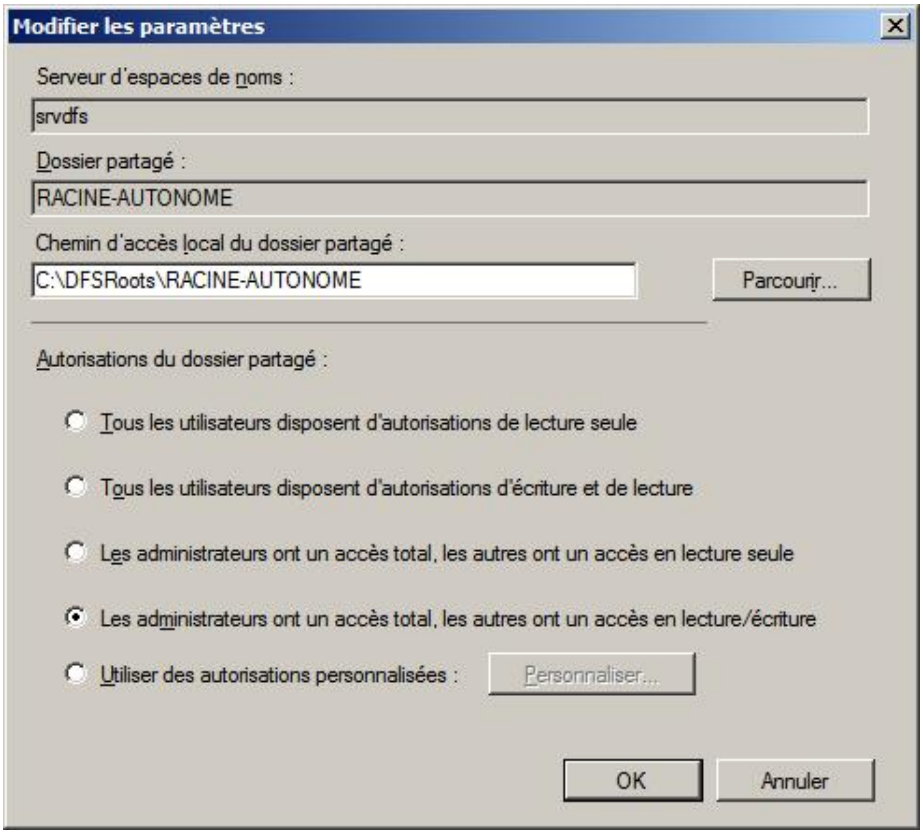

Assistant Nouvel espace de noms
Serveur d'espaces de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Entrez le nom du serveur qui hébergera l'espace de noms. Le serveur spécifié sera reconnu comme le serveur d'espaces de noms.
Serveur :
srvdfs
Parcourir...
Pour plus d'informations sur la configuration requise pour les serveurs d'espace de noms, voir Aide sur la gestion du système de fichiers distribués DFS.
< Précédent
Suivant >
Annuler

- Cliquez sur **Modifier les paramètres** afin d'indiquer les permissions souhaitées sur la racine **RACINE-AUTONOME** qui sera vue comme un partage du serveur correspondant.

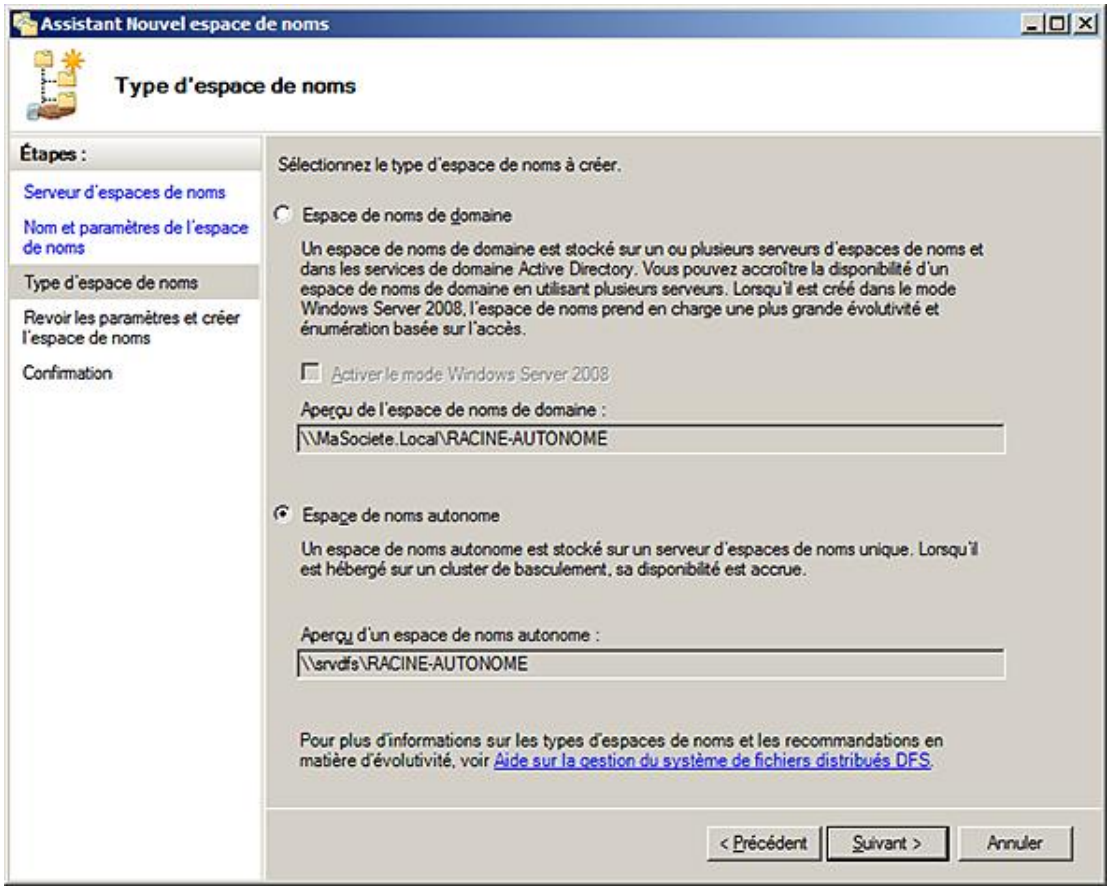

Assistant Nouvel espace de noms
Nom et paramètres de l'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.
Nom :
RACINE-AUTONOME
Exemple : Public
Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.
Modifier les paramètres...
< Précédent
Suivant >
Annuler

© ENI Editions - All rigths reserved

Il faut faire attention aux droits positionnés à ce niveau, car les éléments créés à la racine de ce partage se retrouveront effectivement dans le dossier local indiqué.


Modifier les paramètres
Serveur d'espaces de noms :
srvdfs
Dossier partagé :
RACINE-AUTONOME
Chemin d'accès local du dossier partagé :
C:\DFSRoots\RACINE-AUTONOME
Parcourir...
Autorisations du dossier partagé :
Tous les utilisateurs disposent d'autorisations de lecture seule
Tous les utilisateurs disposent d'autorisations d'écriture et de lecture
Les administrateurs ont un accès total, les autres ont un accès en lecture seule
Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture
Utiliser des autorisations personnalisées :
Personnaliser...
OK
Annuler

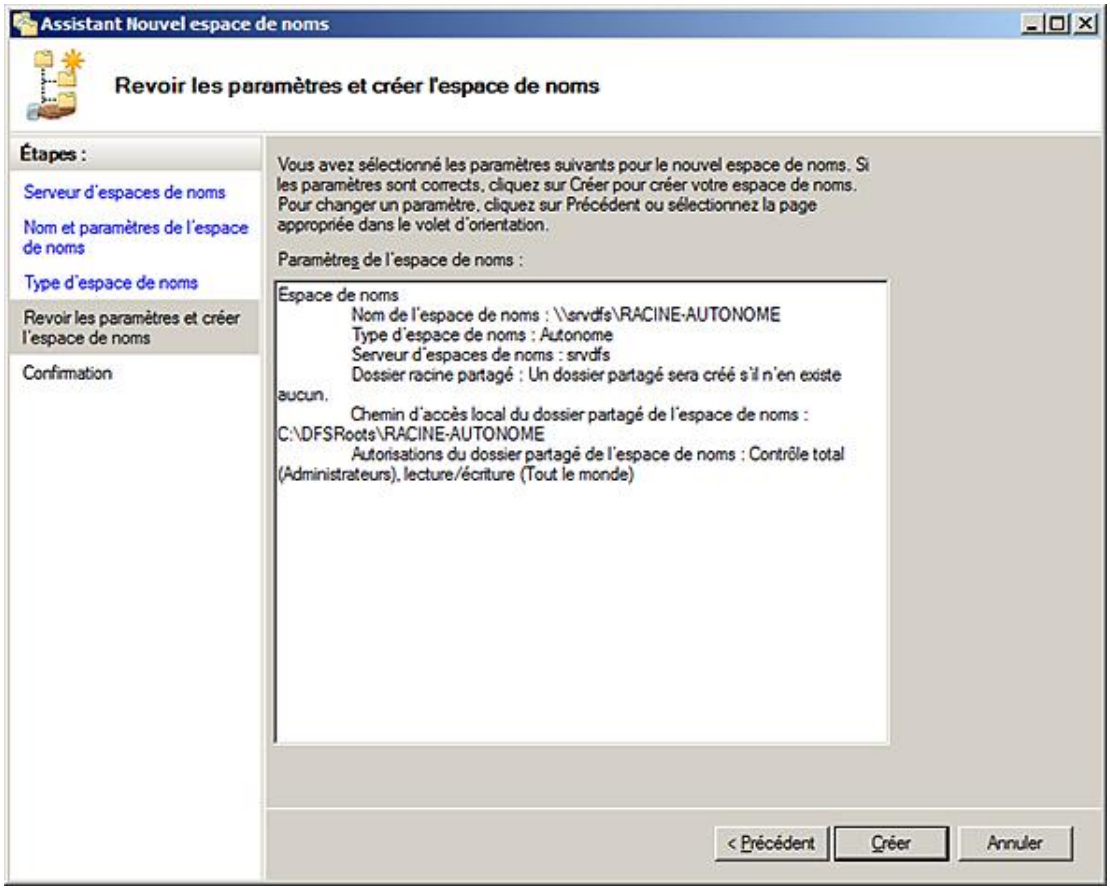
Le type d'espace correspond au choix crucial entre une racine qui sera spécifique à ce serveur, et une racine dite **de noms de domaine** qui pourra être vue et utilisée par toute la forêt. La racine **autonome** ne pourra être vue qu'à partir du serveur qui l'héberge.


Assistant Nouvel espace de noms
Type d'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Sélectionnez le type d'espace de noms à créer.
Espace de noms de domaine
Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande évolutivité et énumération basée sur l'accès.
Activer le mode Windows Server 2008
Aperçu de l'espace de noms de domaine :
\\MaSociete.Local\RACINE-AUTONOME
Espace de noms autonome
Un espace de noms autonome est stocké sur un serveur d'espaces de noms unique. Lorsqu'il est hébergé sur un cluster de basculement, sa disponibilité est accrue.
Aperçu d'un espace de noms autonome :
\\srvdfs\RACINE-AUTONOME
Pour plus d'informations sur les types d'espaces de noms et les recommandations en matière d'évolutivité, voir Aide sur la gestion du système de fichiers distribués DFS.
< Précédent
Suivant >
Annuler

© ENI Editions - All rigths reserved

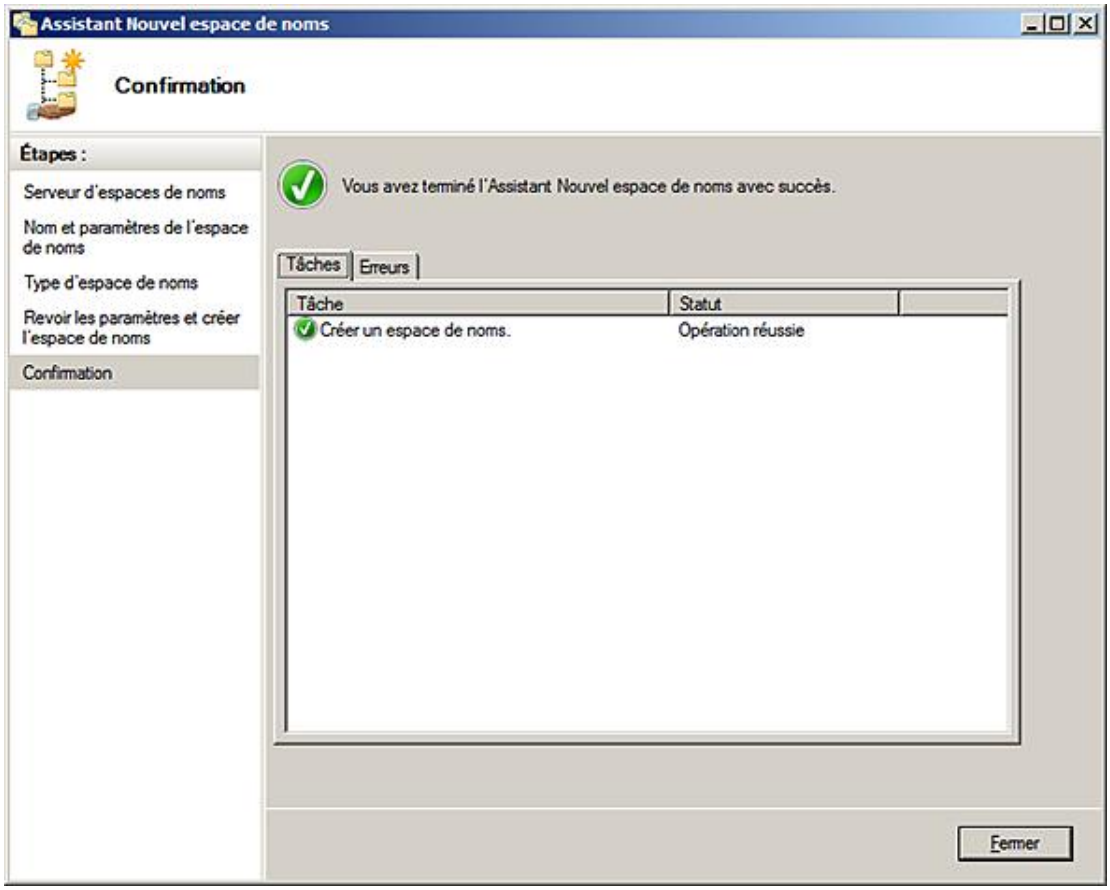
Cet écran reprend tous les choix réalisés.

- Cliquez sur le bouton **Créer**.


Assistant Nouvel espace de noms
Revoir les paramètres et créer l'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Vous avez sélectionné les paramètres suivants pour le nouvel espace de noms. Si les paramètres sont corrects, cliquez sur Créer pour créer votre espace de noms. Pour changer un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.
Paramètres de l'espace de noms :
Espace de noms
Nom de l'espace de noms : \\srvdfs\RACINE-AUTONOME
Type d'espace de noms : Autonome
Serveur d'espaces de noms : srvdfs
Dossier racine partagé : Un dossier partagé sera créé s'il n'en existe aucun.
Chemin d'accès local du dossier partagé de l'espace de noms : C:\DFSRoots\RACINE-AUTONOME
Autorisations du dossier partagé de l'espace de noms : Contrôle total (Administrateurs), lecture/écriture (Tout le monde)
< Précédent
Créer
Annuler

Cet écran confirme la création de la racine DFS. L'onglet **Erreurs** donne accès aux erreurs éventuelles. Les journaux d'évènements donneront des informations complémentaires.

© ENI Editions - All rigths reserved



b. Les racines de noms de domaine

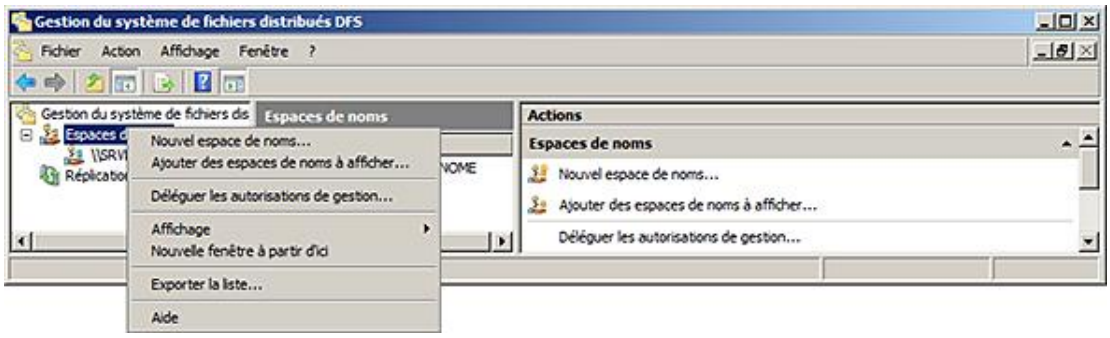
Les racines de noms de domaine sont basées sur la résolution DNS du domaine. L'avantage principal de cette solution réside dans la tolérance de panne qui peut être apportée à la racine par l'utilisation d'au moins deux serveurs liés au niveau de la même racine.

Les racines sont inscrites dans l'Active Directory, ce qui permet aux administrateurs et aux utilisateurs de toute la forêt d'accéder facilement aux unités DFS.

Voici la procédure de création d'une racine de noms de domaine.

Le début de la création est identique à la racine autonome.

- Lancez l'assistant de création d'un **Nouvel espace de noms**.

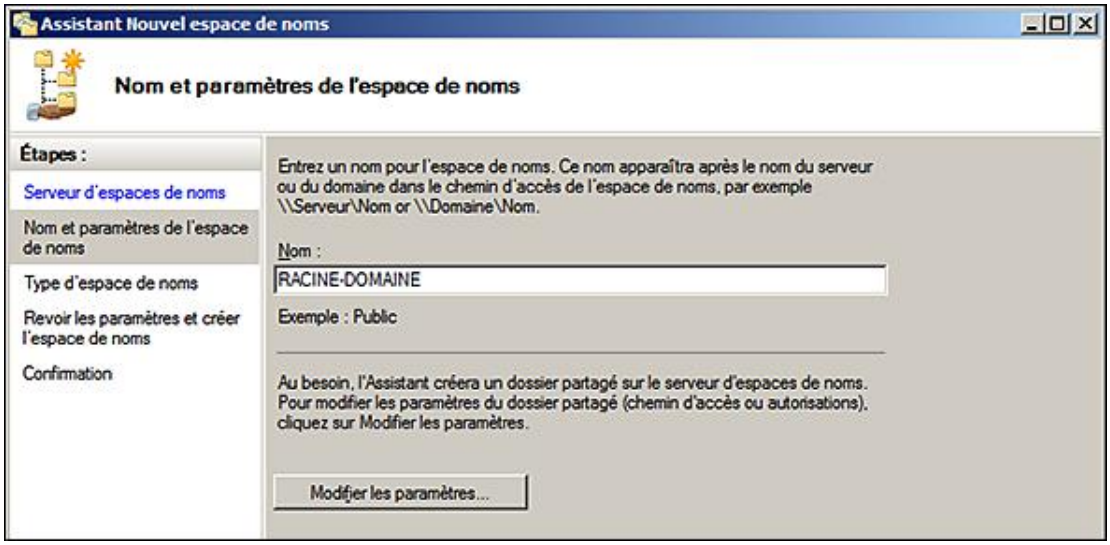


- Indiquez le serveur qui gérera cette racine.

© ENI Editions - All rigths reserved

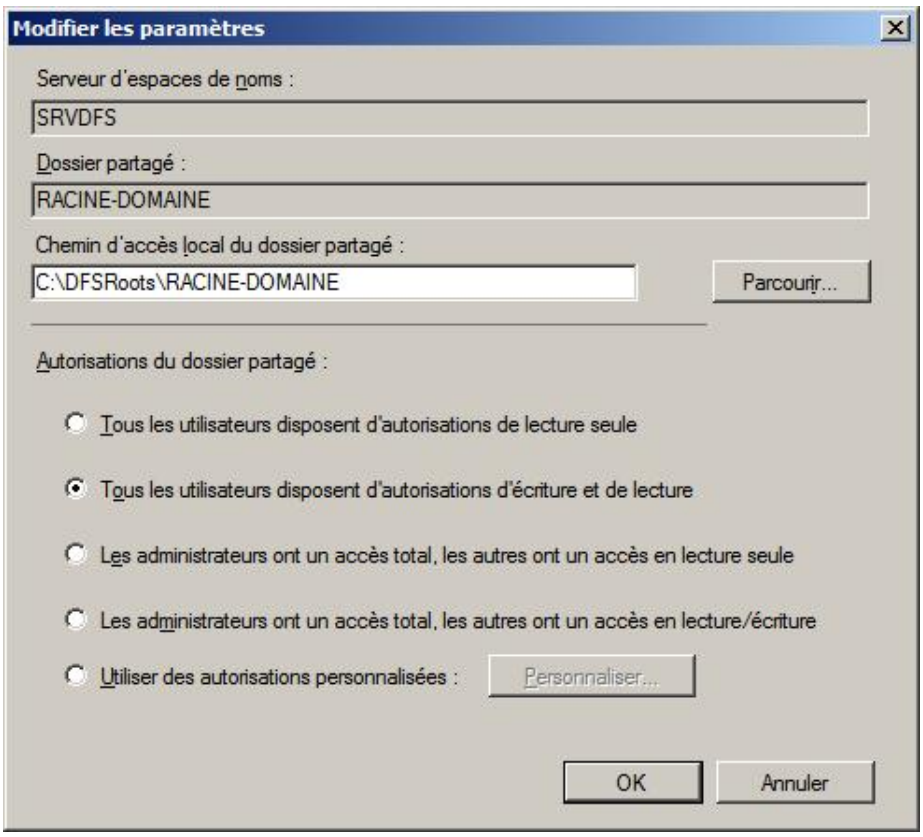
Assistant Nouvel espace de noms
Serveur d'espaces de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Entrez le nom du serveur qui hébergera l'espace de noms. Le serveur spécifié sera reconnu comme le serveur d'espaces de noms.
Serveur :
SRVDFS
Parcourir...

- Indiquez le **Nouvel espace de noms**, sachant que le nom devra être choisi judicieusement car il sera vu et utilisé par tous les utilisateurs de la forêt, voire plus.

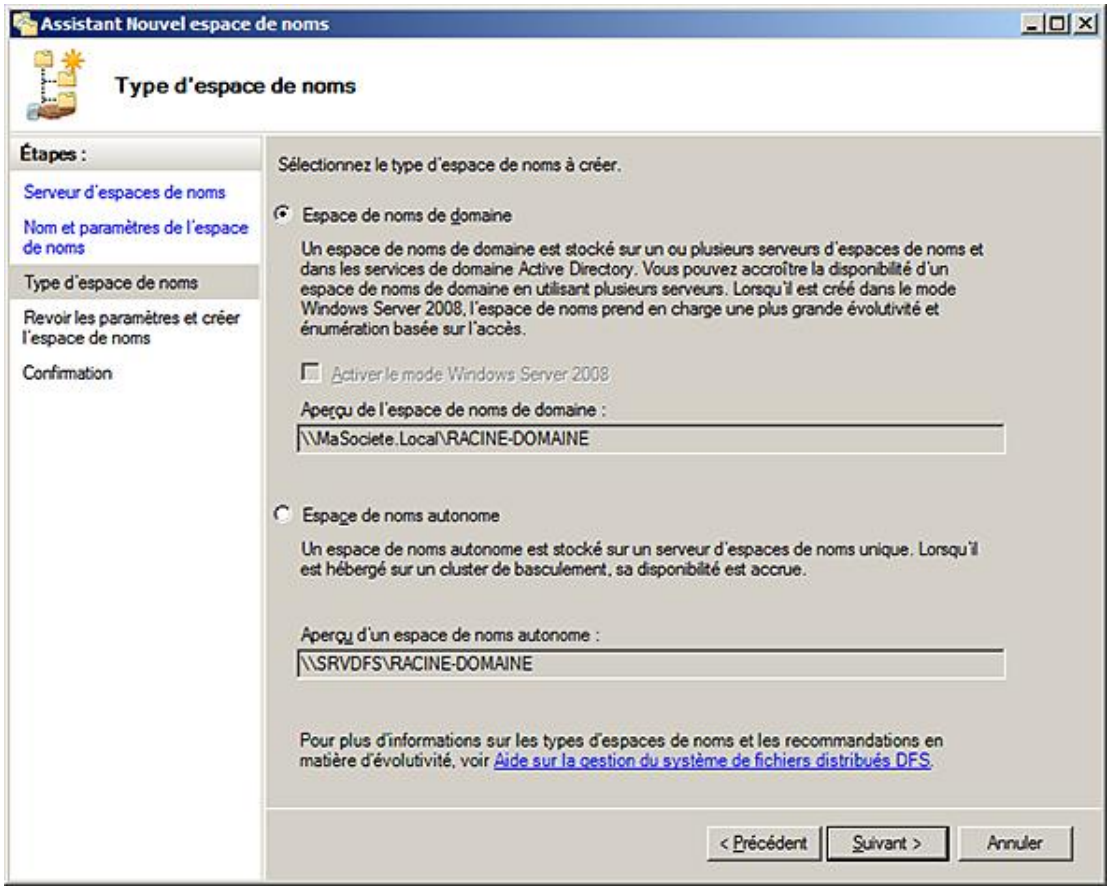

Assistant Nouvel espace de noms
Nom et paramètres de l'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Entrez un nom pour l'espace de noms. Ce nom apparaîtra après le nom du serveur ou du domaine dans le chemin d'accès de l'espace de noms, par exemple \\Serveur\Nom or \\Domaine\Nom.
Nom :
RACINE-DOMAINE
Exemple : Public
Au besoin, l'Assistant créera un dossier partagé sur le serveur d'espaces de noms. Pour modifier les paramètres du dossier partagé (chemin d'accès ou autorisations), cliquez sur Modifier les paramètres.
Modifier les paramètres...

On retrouve les paramètres d'autorisations sur la racine.

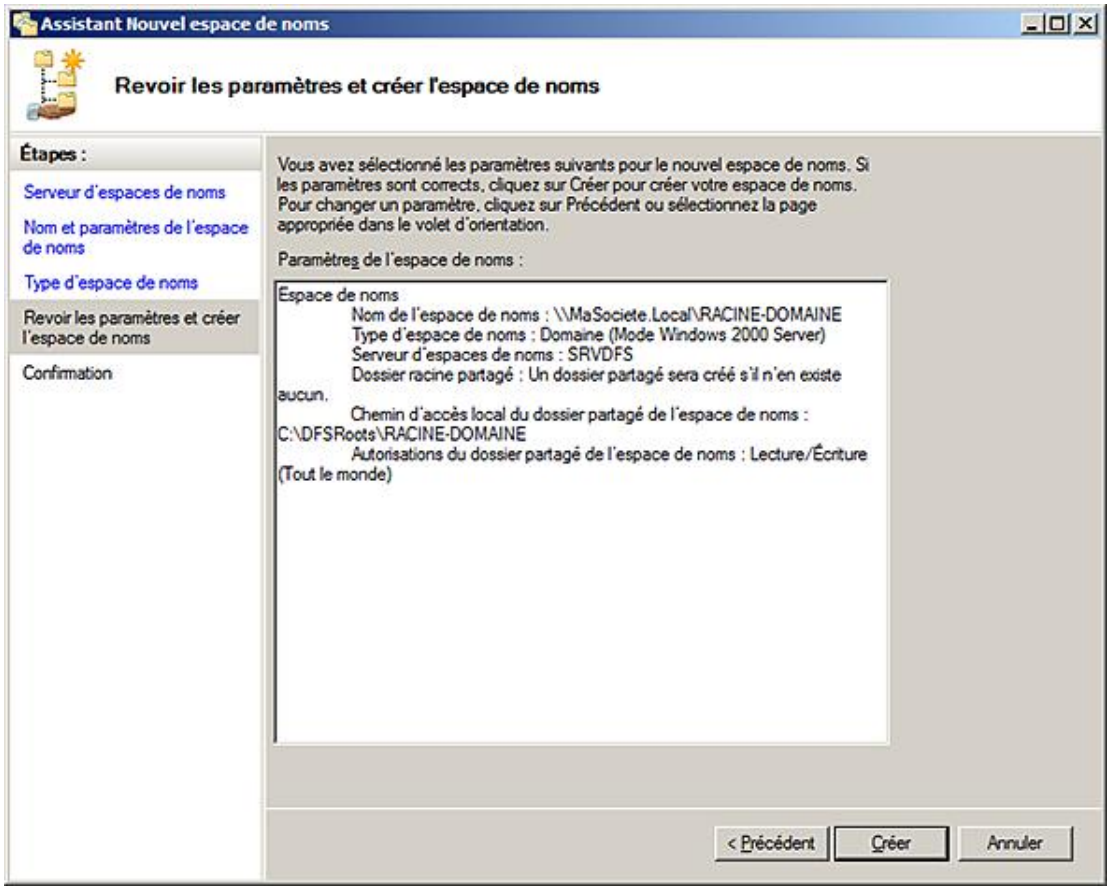
© ENI Editions - All rigths reserved


Modifier les paramètres
Serveur d'espaces de noms :
SRVDFS
Dossier partagé :
RACINE-DOMAINE
Chemin d'accès local du dossier partagé :
C:\DFSRoots\RACINE-DOMAINE
Parcourir...
Autorisations du dossier partagé :
Tous les utilisateurs disposent d'autorisations de lecture seule
Tous les utilisateurs disposent d'autorisations d'écriture et de lecture
Les administrateurs ont un accès total, les autres ont un accès en lecture seule
Les administrateurs ont un accès total, les autres ont un accès en lecture/écriture
Utiliser des autorisations personnalisées :
Personnaliser...
OK
Annuler

L'espace de noms de domaine permet de se baser sur la résolution du nom de domaine pour accéder à un espace partagé facile à trouver.


Assistant Nouvel espace de noms
Type d'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Sélectionnez le type d'espace de noms à créer.
Espace de noms de domaine
Un espace de noms de domaine est stocké sur un ou plusieurs serveurs d'espaces de noms et dans les services de domaine Active Directory. Vous pouvez accroître la disponibilité d'un espace de noms de domaine en utilisant plusieurs serveurs. Lorsqu'il est créé dans le mode Windows Server 2008, l'espace de noms prend en charge une plus grande évolutivité et énumération basée sur l'accès.
Activer le mode Windows Server 2008
Aperçu de l'espace de noms de domaine :
\\MaSociete.Local\RACINE-DOMAINE
Espace de noms autonome
Un espace de noms autonome est stocké sur un serveur d'espaces de noms unique. Lorsqu'il est hébergé sur un cluster de basculement, sa disponibilité est accrue.
Aperçu d'un espace de noms autonome :
\\SRVDFS\RACINE-DOMAINE
Pour plus d'informations sur les types d'espaces de noms et les recommandations en matière d'évolutivité, voir Aide sur la gestion du système de fichiers distribués DFS.
< Précédent
Suivant >
Annuler

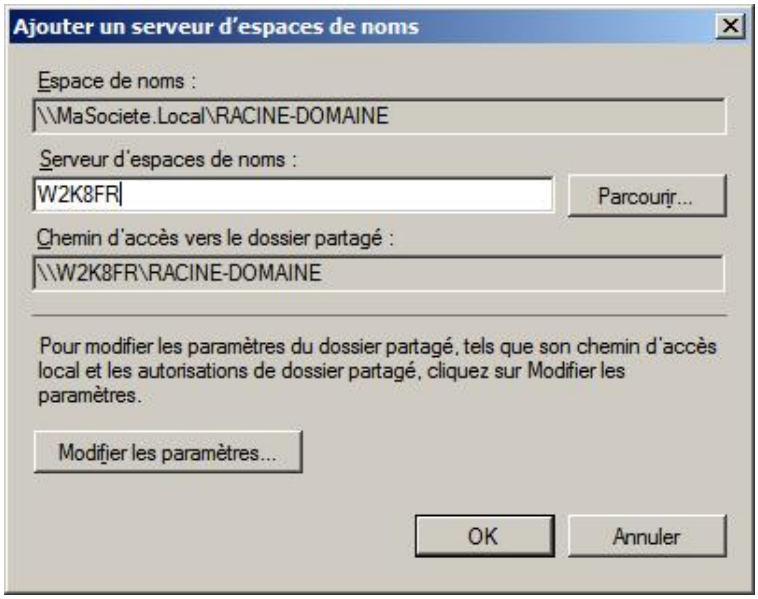
© ENI Editions - All rigths reserved


Assistant Nouvel espace de noms
Revoir les paramètres et créer l'espace de noms
Étapes :
Serveur d'espaces de noms
Nom et paramètres de l'espace de noms
Type d'espace de noms
Revoir les paramètres et créer l'espace de noms
Confirmation
Vous avez sélectionné les paramètres suivants pour le nouvel espace de noms. Si les paramètres sont corrects, cliquez sur Créer pour créer votre espace de noms. Pour changer un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.
Paramètres de l'espace de noms :
Espace de noms
Nom de l'espace de noms : \\MaSociete.Local\RACINE-DOMAINE
Type d'espace de noms : Domaine (Mode Windows 2000 Server)
Serveur d'espaces de noms : SRVDFS
Dossier racine partagé : Un dossier partagé sera créé s'il n'en existe aucun.
Chemin d'accès local du dossier partagé de l'espace de noms : C:\DFSRoots\RACINE-DOMAINE
Autorisations du dossier partagé de l'espace de noms : Lecture/Écriture (Tout le monde)
< Précédent
Créer
Annuler

À noter que la création de la racine de domaine sera liée au mode de fonctionnement du domaine qui l'héberge.

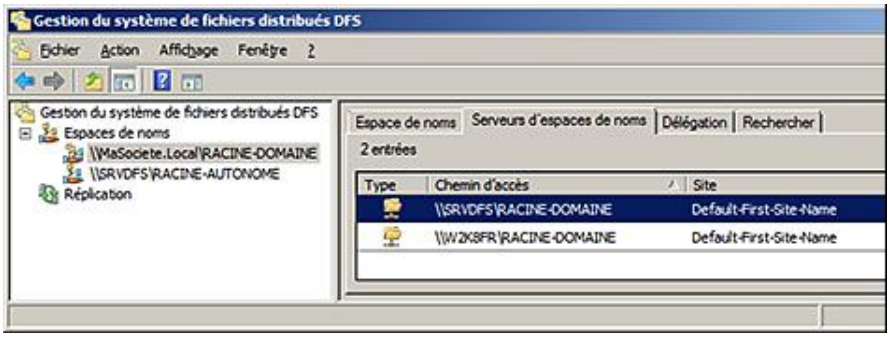
L'utilisation d'une racine de domaine suppose que l'on veut utiliser la tolérance aux pannes et l'équilibrage de charge sur la racine de DFS. Ceci est obtenu par l'ajout d'un serveur d'espace de noms supplémentaire.

Vous pouvez sélectionner ou saisir directement le nouveau nom du serveur à utiliser.


Ajouter un serveur d'espaces de noms
Espace de noms :
\\MaSociete.Local\RACINE-DOMAINE
Serveur d'espaces de noms :
W2K8FR
Parcourir...
Chemin d'accès vers le dossier partagé :
\\W2K8FR\RACINE-DOMAINE
Pour modifier les paramètres du dossier partagé, tels que son chemin d'accès local et les autorisations de dossier partagé, cliquez sur Modifier les paramètres.
Modifier les paramètres...
OK
Annuler

Bien entendu, il peut y avoir plus de deux serveurs contenant l'information sur les DFS.

© ENI Editions - All rigths reserved



2. La création des liaisons DFS et cibles DFS

Le nom d'une liaison correspond au nom de dossier qui apparaît dans l'espace de nom distribué. Une cible DFS correspond à un chemin réseau, c'est-à-dire un partage situé sur n'importe quel serveur (ou station du domaine) et que l'on associe à une liaison DFS.

Une liaison DFS peut être associée à plusieurs cibles, donc plusieurs partages différents. Il sera alors nécessaire de configurer la réplication de ces dossiers afin d'obtenir un contenu identique et synchronisé entre les différentes cibles.

Voici la procédure pour définir une cible sur les partages COMPTA1 et COMPTA2 définis sur deux serveurs différents :

- Sélectionnez l'espace de noms souhaité (Autonome ou de domaine), puis utilisez le clic droit pour afficher le menu.
- Utilisez l'option **Nouveau Dossier**.
- Saisissez le nom de la liaison DFS **COMPTA**.
- Cliquez sur **Ajouter** pour ajouter les cibles associées à cette liaison.
- Vous pouvez saisir directement le nom UNC d'accès à la ressource sous la forme \\SERVEUR\PARTAGE ou cliquez sur **Parcourir**.

  Dans le deuxième cas, l'astuce est d'indiquer le nom du serveur, puis de cliquer sur le bouton **Afficher les dossiers partagés**.
- Si plusieurs cibles sont précisées, l'assistant vous propose de créer un groupe de réplication, l'assistant de création d'un groupe de réplication est alors lancé automatiquement.

La procédure de mise en place d'une réplication est décrite dans la section suivante.

3. La réplication

La réplication est basée sur un moteur multimaître qui permet donc de prendre en compte les modifications simultanées de fichiers provenant de plusieurs points différents et de synchroniser l'ensemble. Cette réplication s'adapte aux liaisons lentes par l'utilisation d'une technologie de compression différentielle appelée **RDC**.

Chaque groupe de réplication (ensemble de serveurs) peut prendre en charge plusieurs dossiers répliqués.

Chaque dossier répliqué peut avoir ses propres paramètres, notamment des filtres de réplication permettant de limiter les types de fichiers et les sous-dossiers à inclure dans la réplication.

a. Les filtres de réplication

Par défaut, les filtres de fichiers excluent les fichiers temporaires commençant par le caractère ~ ainsi que les extensions .BAK et .TMP.

Par ailleurs, les fichiers suivants sont toujours exclus :

© ENI Editions - All rigths reserved

- les points de montages NTFS ;
- les fichiers chiffrés par EFS ;
- les fichiers définis comme temporaires.

Les dossiers comme les fichiers peuvent être exclus à partir de leurs noms. Il est possible d'utiliser le caractère générique *.

Les bases de données, les fichiers vidéo et les images de CD peuvent ainsi être exclus de cette réplication.

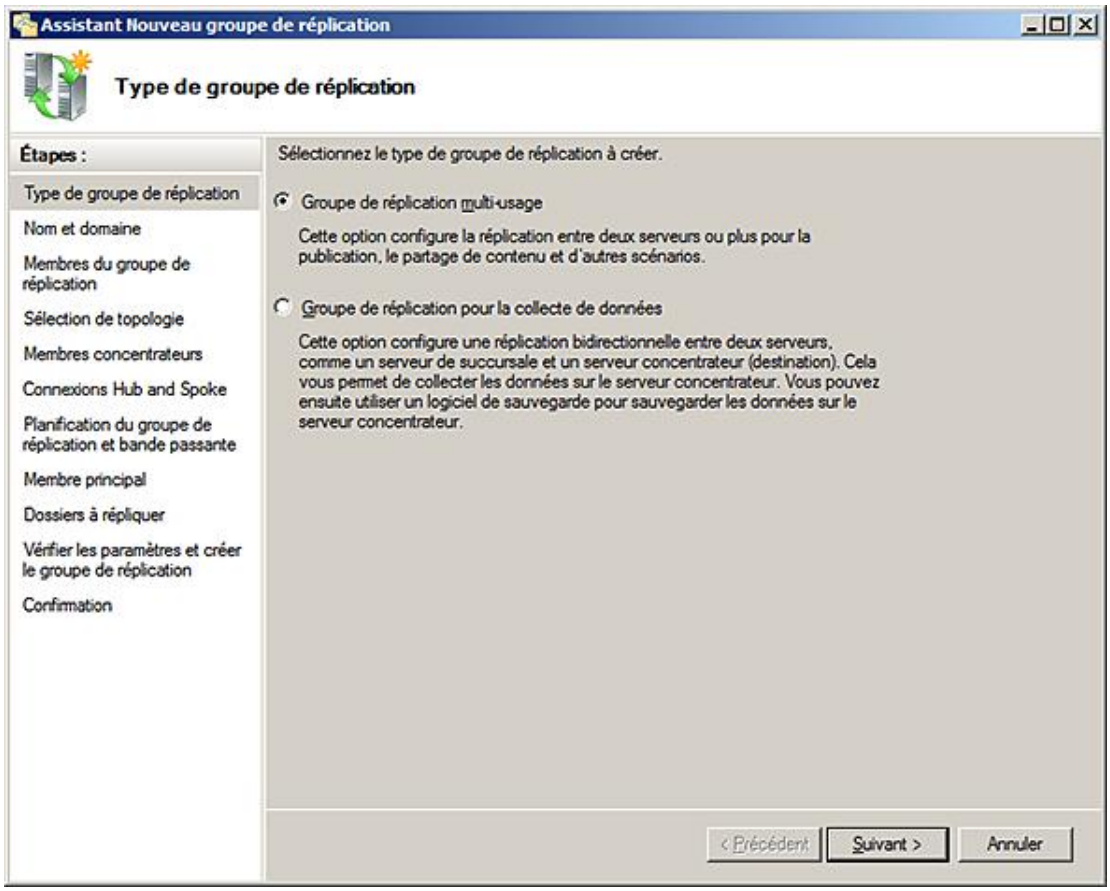
b. La mise en place graphique de la réplication

Voici la procédure graphique de mise en place d'une réplication.

Cette réplication se met en place de la même manière sur une racine autonome ou de domaine.

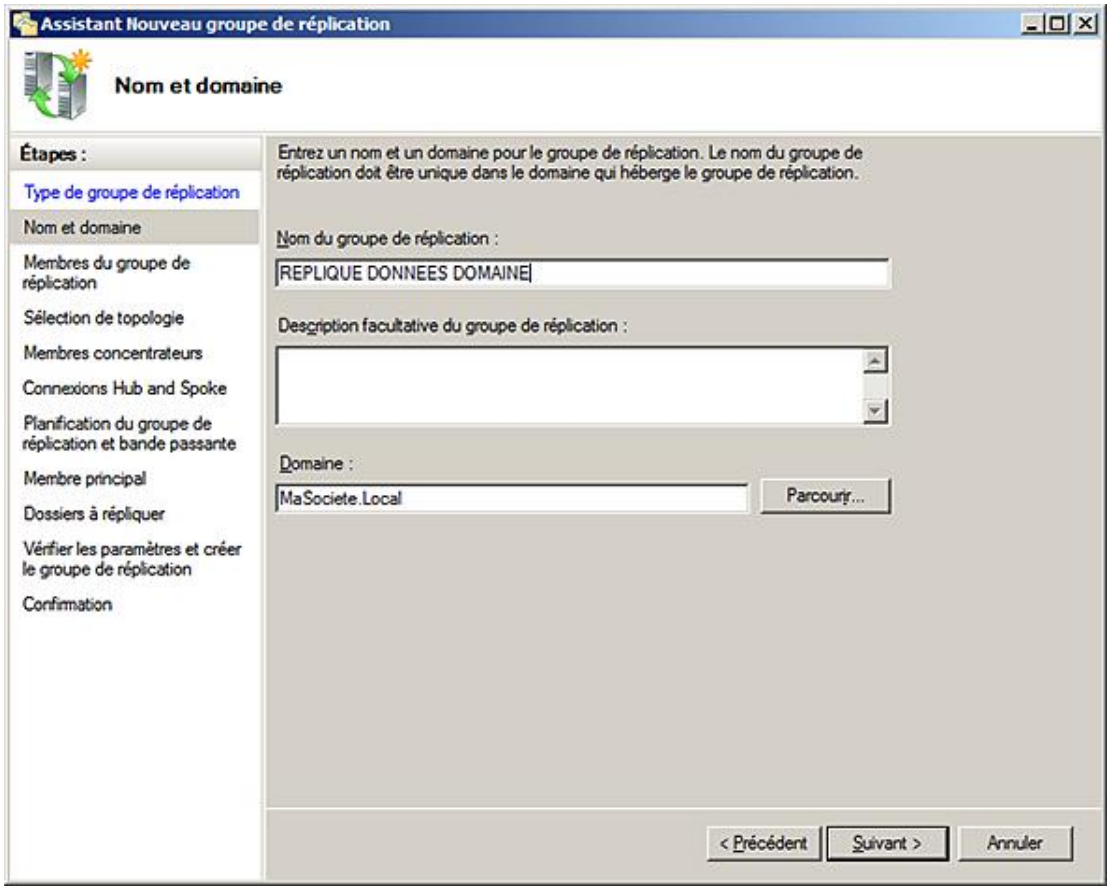
- Sélectionnez le module **Réplication**, puis cliquez avec le bouton droit pour faire apparaître le menu. Choisissez l'option **Nouveau groupe de réplication**.

Ce choix permet principalement de définir si la réplication sera liée uniquement à deux serveurs, dont l'un contiendra les données principales.

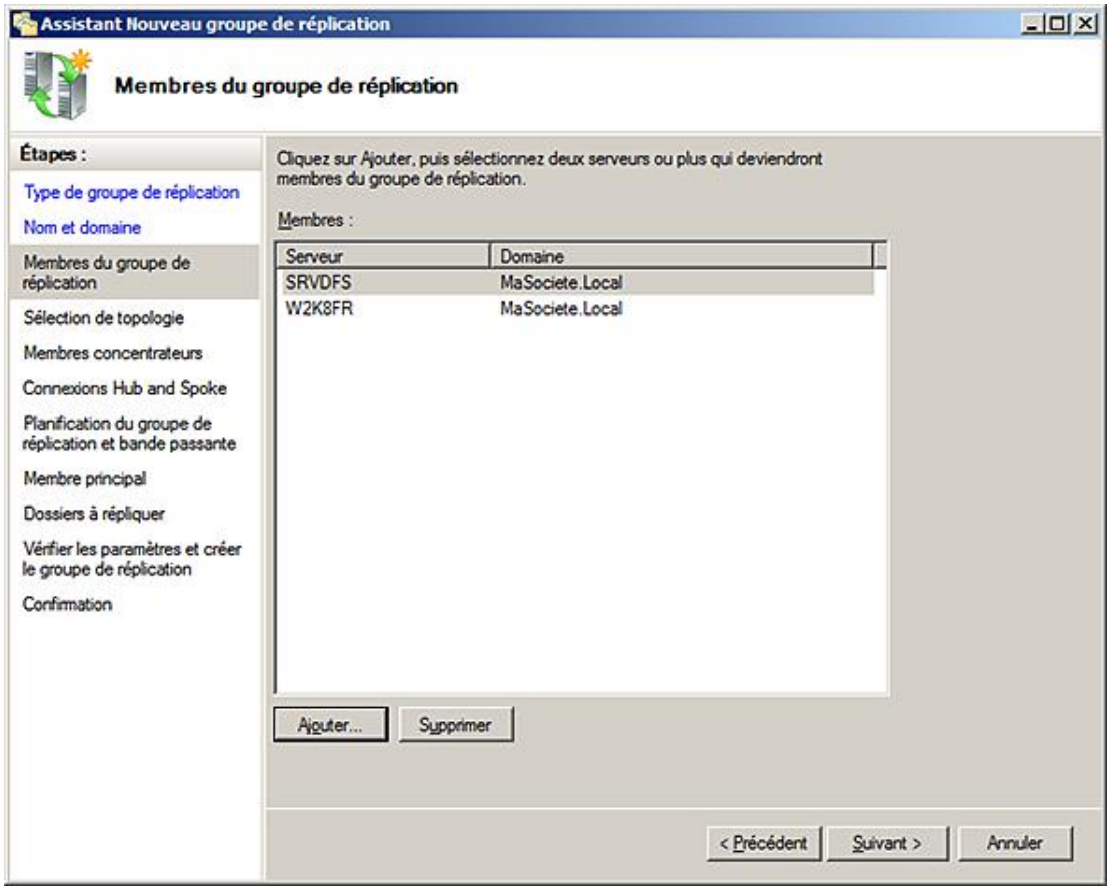

Assistant Nouveau groupe de réplication
Type de groupe de réplication
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Membres concentrateurs
Connexions Hub and Spoke
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Sélectionnez le type de groupe de réplication à créer.
Groupe de réplication multi-usage
Cette option configure la réplication entre deux serveurs ou plus pour la publication, le partage de contenu et d'autres scénarios.
Groupe de réplication pour la collecte de données
Cette option configure une réplication bidirectionnelle entre deux serveurs, comme un serveur de succursale et un serveur concentrateur (destination). Cela vous permet de collecter les données sur le serveur concentrateur. Vous pouvez ensuite utiliser un logiciel de sauvegarde pour sauvegarder les données sur le serveur concentrateur.
< Précédent
Suivant >
Annuler

- Nommez la réplication.

© ENI Editions - All rigths reserved

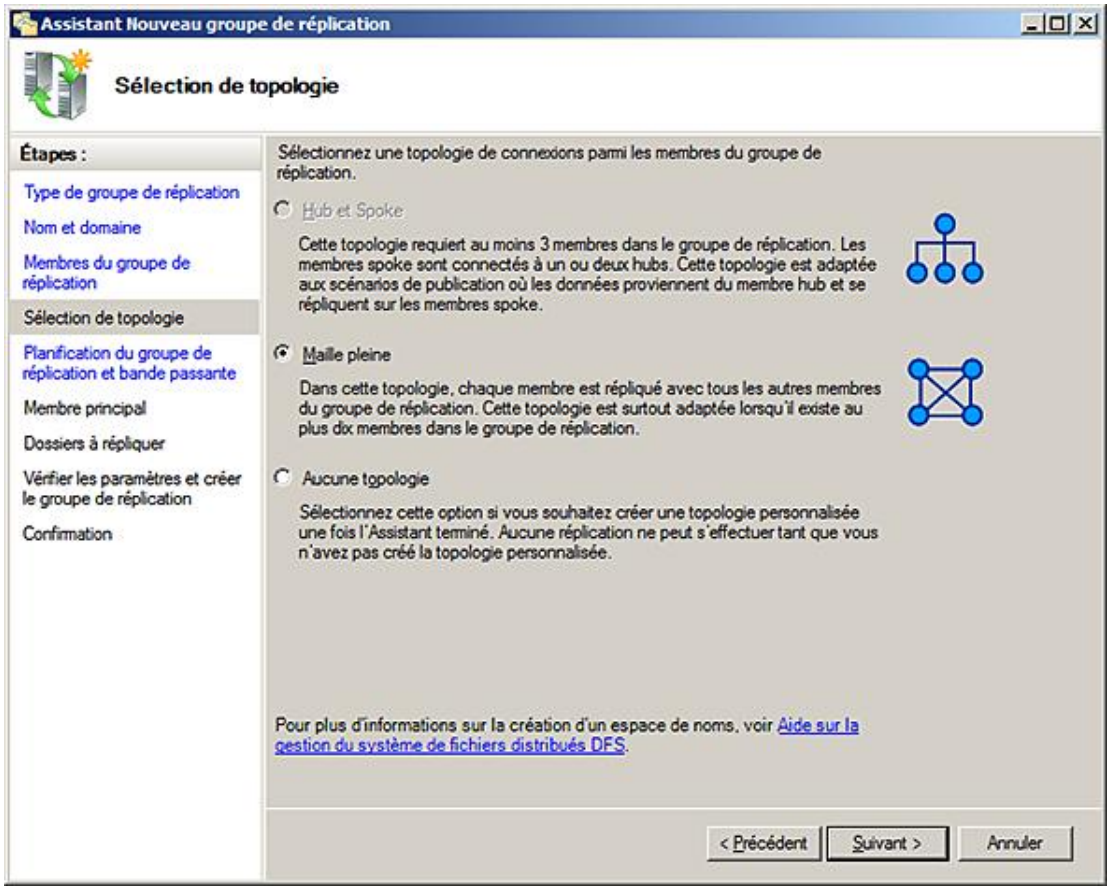

Assistant Nouveau groupe de réplication
Nom et domaine
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Membres concentrateurs
Connexions Hub and Spoke
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Entrez un nom et un domaine pour le groupe de réplication. Le nom du groupe de réplication doit être unique dans le domaine qui héberge le groupe de réplication.
Nom du groupe de réplication :
REPLIQUE DONNEES DOMAINE
Description facultative du groupe de réplication :
Domaine :
MaSociete.Local
Parcourir...
< Précédent
Suivant >
Annuler

- Indiquez les serveurs membres.

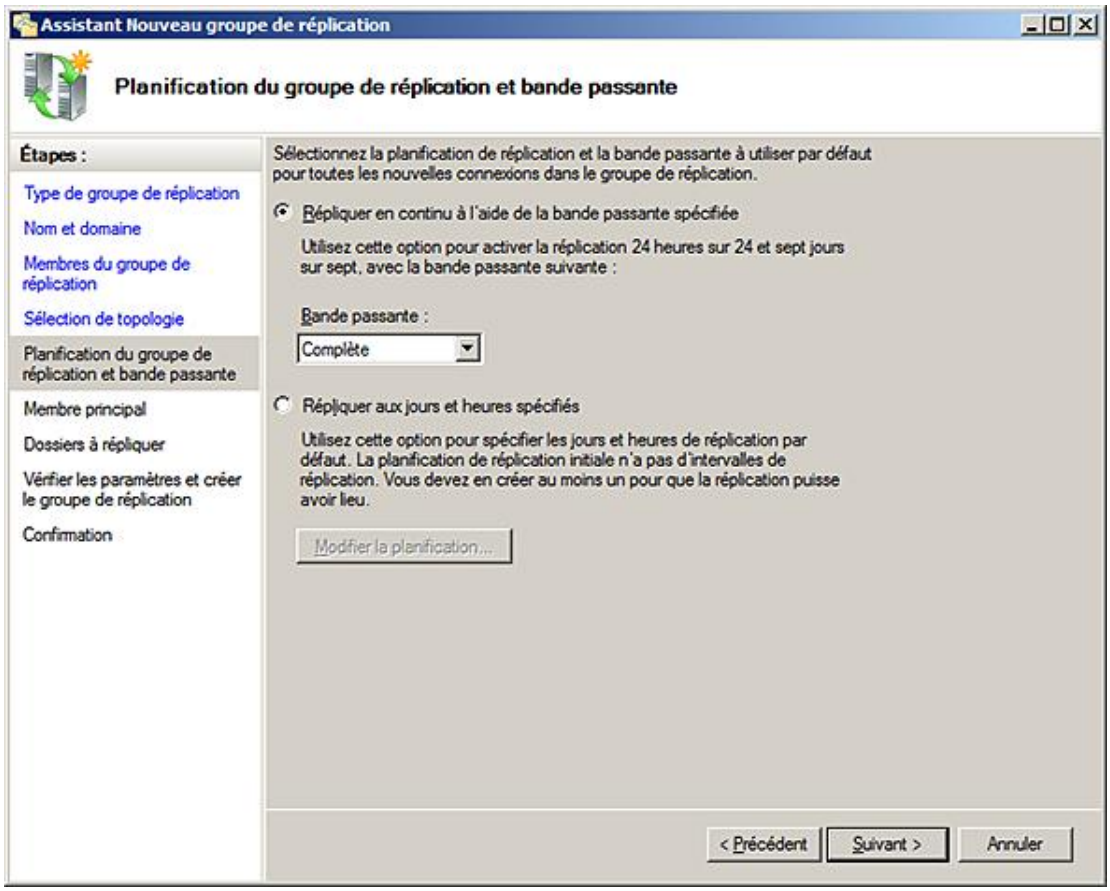


© ENI Editions - All rigths reserved

- Choisissez la topologie la plus adaptée à vos besoins. La topologie en maille pleine est adaptée aux modifications autorisées provenant de tous les serveurs membres.


Assistant Nouveau groupe de réplication
Sélection de topologie
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Sélectionnez une topologie de connexions parmi les membres du groupe de réplication.
Hub et Spoke
Cette topologie requiert au moins 3 membres dans le groupe de réplication. Les membres spoke sont connectés à un ou deux hubs. Cette topologie est adaptée aux scénarios de publication où les données proviennent du membre hub et se répliquent sur les membres spoke.
Maille pleine
Dans cette topologie, chaque membre est répliqué avec tous les autres membres du groupe de réplication. Cette topologie est surtout adaptée lorsqu'il existe au plus dix membres dans le groupe de réplication.
Aucune topologie
Sélectionnez cette option si vous souhaitez créer une topologie personnalisée une fois l'Assistant terminé. Aucune réplication ne peut s'effectuer tant que vous n'avez pas créé la topologie personnalisée.
Pour plus d'informations sur la création d'un espace de noms, voir Aide sur la gestion du système de fichiers distribués DFS.
< Précédent
Suivant >
Annuler

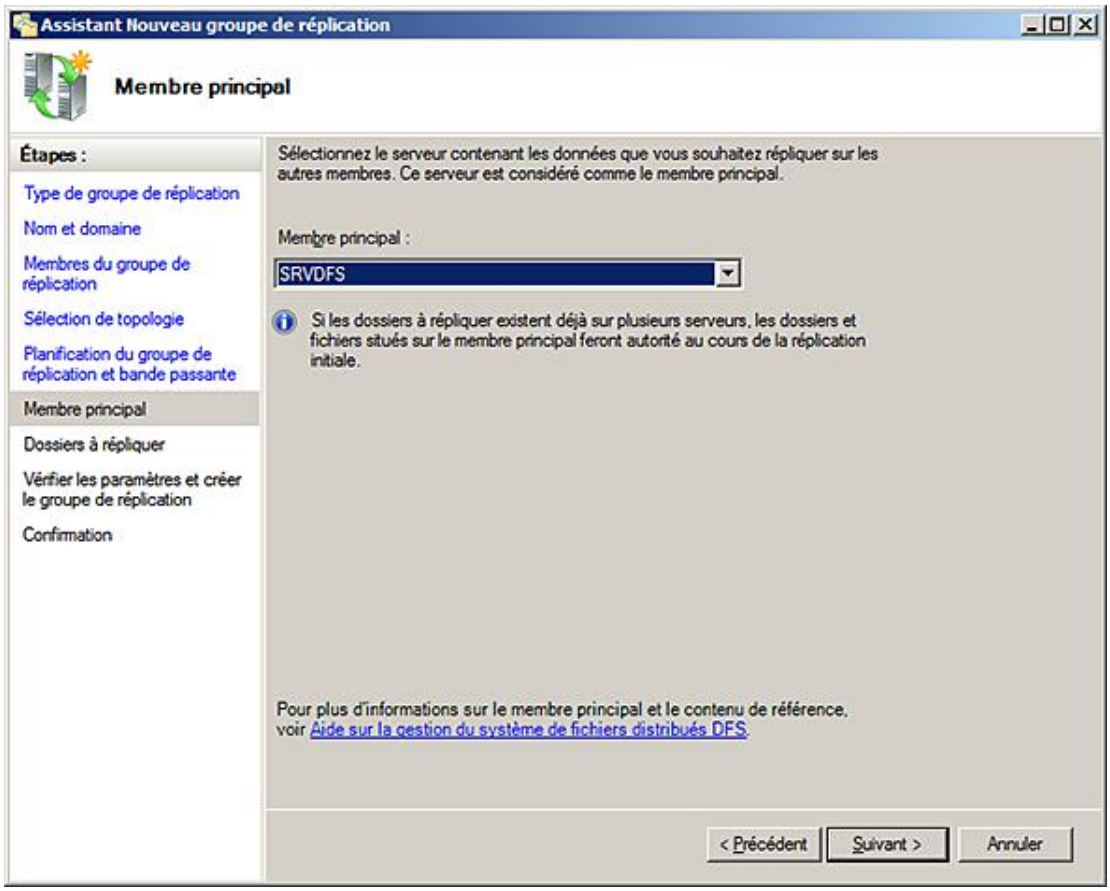
Selon les possibilités de votre réseau, il sera possible de moduler les horaires et le taux d'utilisation du réseau.


Assistant Nouveau groupe de réplication
Planification du groupe de réplication et bande passante
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Sélectionnez la planification de réplication et la bande passante à utiliser par défaut pour toutes les nouvelles connexions dans le groupe de réplication.
Répliquer en continu à l'aide de la bande passante spécifiée
Utilisez cette option pour activer la réplication 24 heures sur 24 et sept jours sur sept, avec la bande passante suivante :
Bande passante :
Complète
Répliquer aux jours et heures spécifiés
Utilisez cette option pour spécifier les jours et heures de réplication par défaut. La planification de réplication initiale n'a pas d'intervalles de réplication. Vous devez en créer au moins un pour que la réplication puisse avoir lieu.
Modifier la planification...
< Précédent
Suivant >
Annuler

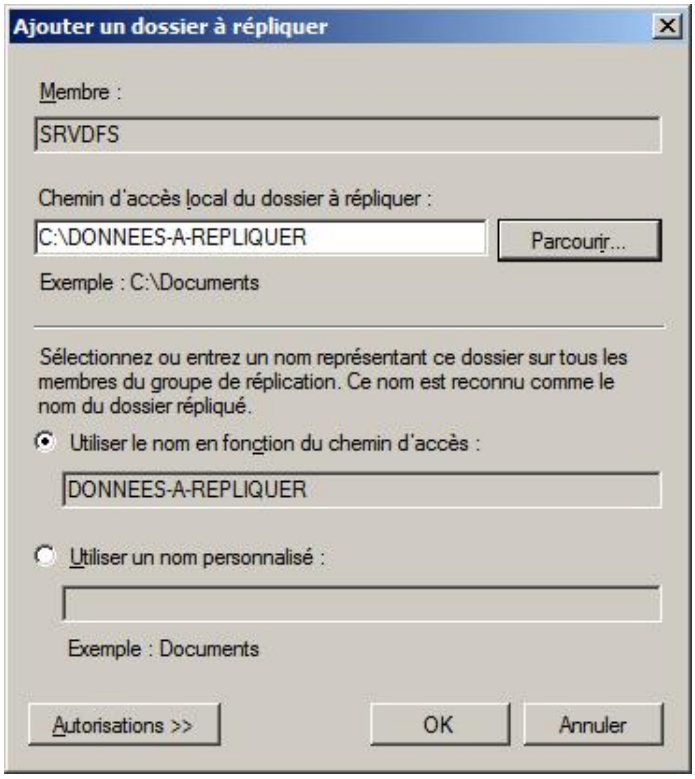
© ENI Editions - All rigths reserved

Vous pourrez modifier facilement les paramètres de réplication par la suite.

Il est préférable de démarrer les réplications sur des dossiers vides. Sinon, cette option permet de définir le serveur contenant les données initiales.

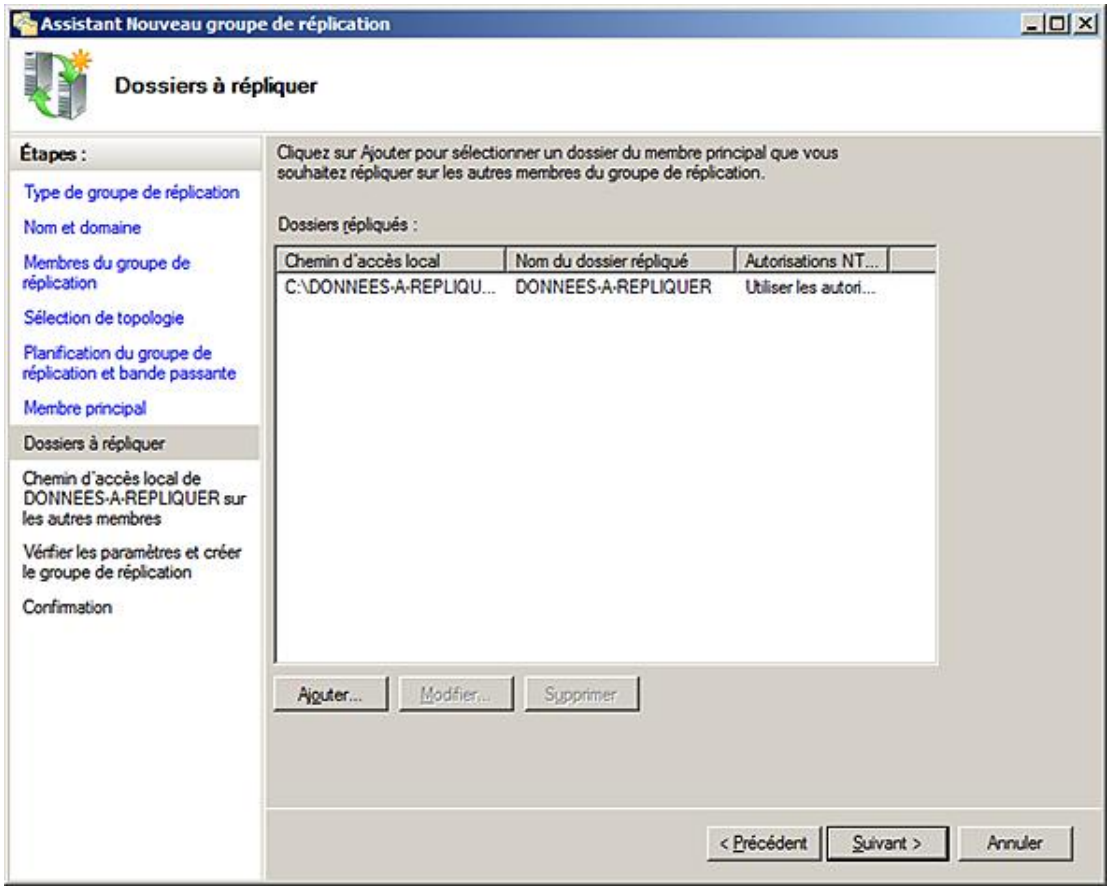

Assistant Nouveau groupe de réplication
Membre principal
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Sélectionnez le serveur contenant les données que vous souhaitez répliquer sur les autres membres. Ce serveur est considéré comme le membre principal.
Membre principal :
SRVDFS
Si les dossiers à répliquer existent déjà sur plusieurs serveurs, les dossiers et fichiers situés sur le membre principal feront autorité au cours de la réplication initiale.
Pour plus d'informations sur le membre principal et le contenu de référence, voir Aide sur la gestion du système de fichiers distribués DFS.
< Précédent
Suivant >
Annuler

- Indiquez le nom exact du dossier racine à répliquer.


Ajouter un dossier à répliquer
Membre :
SRVDFS
Chemin d'accès local du dossier à répliquer :
C:\DONNEES-A-REPLIQUER
Parcourir...
Exemple : C:\Documents
Sélectionnez ou entrez un nom représentant ce dossier sur tous les membres du groupe de réplication. Ce nom est reconnu comme le nom du dossier répliqué.
Utiliser le nom en fonction du chemin d'accès :
DONNEES-A-REPLIQUER
Utiliser un nom personnalisé :
Exemple : Documents
Autorisations >>
OK
Annuler

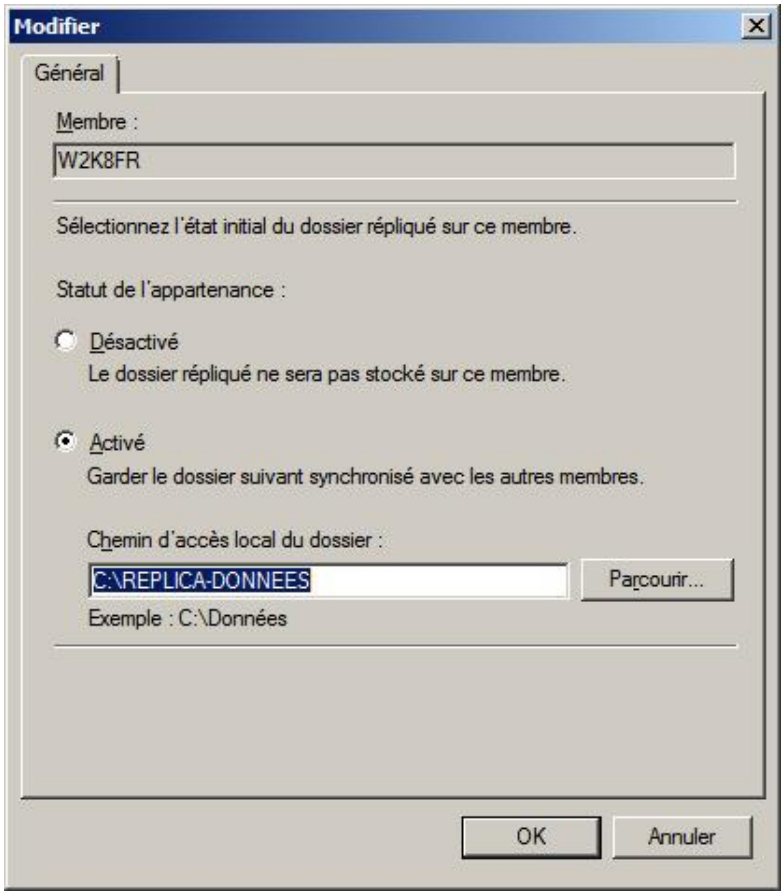
© ENI Editions - All rigths reserved

D’autres dossiers peuvent être ajoutés à ce groupe de réplication immédiatement ou par la suite !

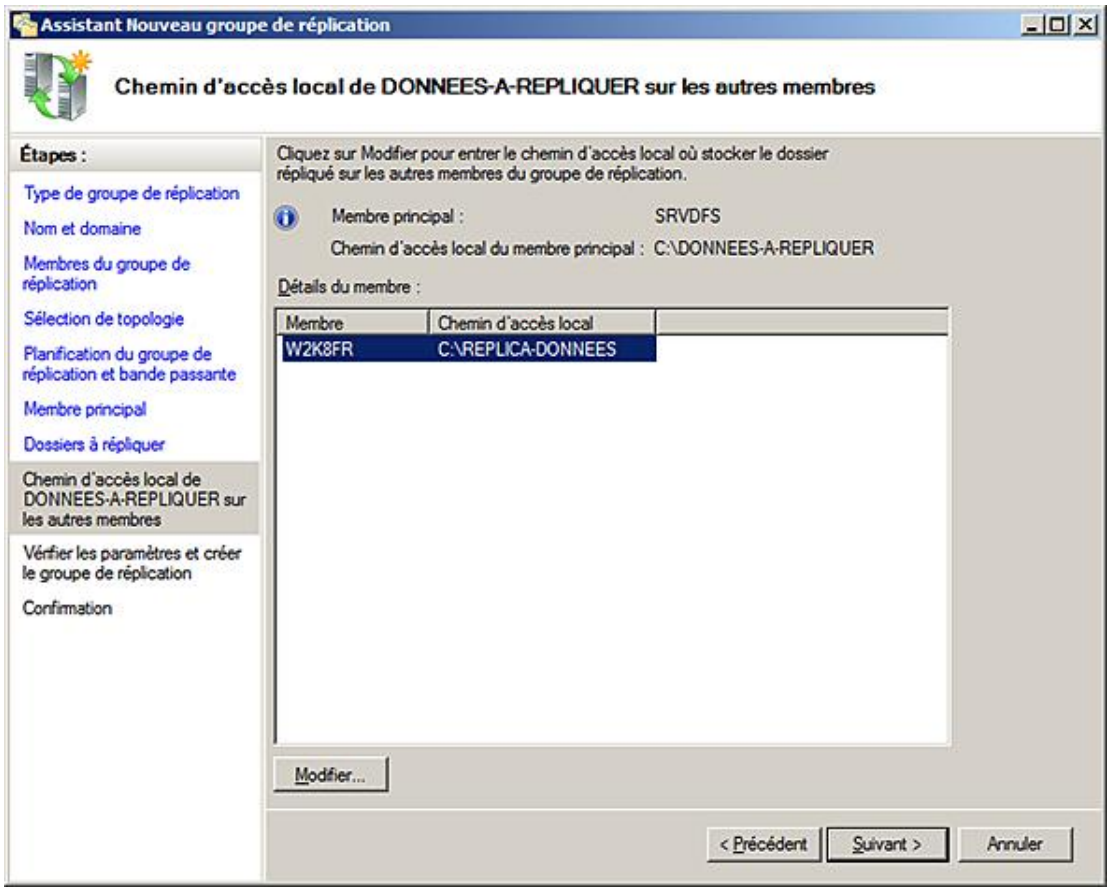

Assistant Nouveau groupe de réplication
Dossiers à répliquer
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Chemin d'accès local de DONNEES-A-REPLIQUER sur les autres membres
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Cliquez sur Ajouter pour sélectionner un dossier du membre principal que vous souhaitez répliquer sur les autres membres du groupe de réplication.
Dossiers répliqués :
Chemin d'accès local
Nom du dossier répliqué
Autorisations NT...
C:\DONNEES-A-REPLIQU...
DONNEES-A-REPLIQUER
Utiliser les autori...
Ajouter...
Modifier...
Supprimer
< Précédent
Suivant >
Annuler

- Pour chaque serveur contenant un réplica des données, activez la réplication en indiquant un dossier de destination. Sélectionnez le serveur, puis le bouton **Modifier**.

© ENI Editions - All rigths reserved

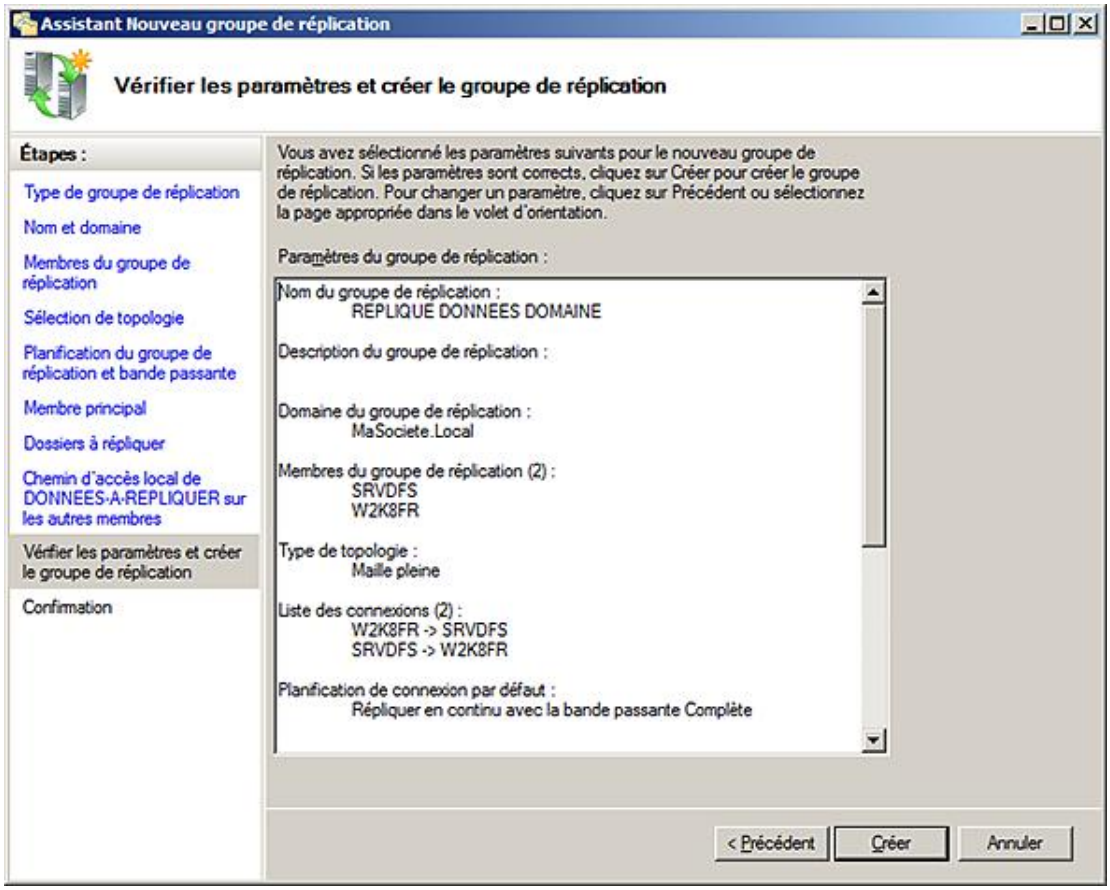


Cette option permet d'indiquer de créer le dossier principal contenant les dossiers répliqués.

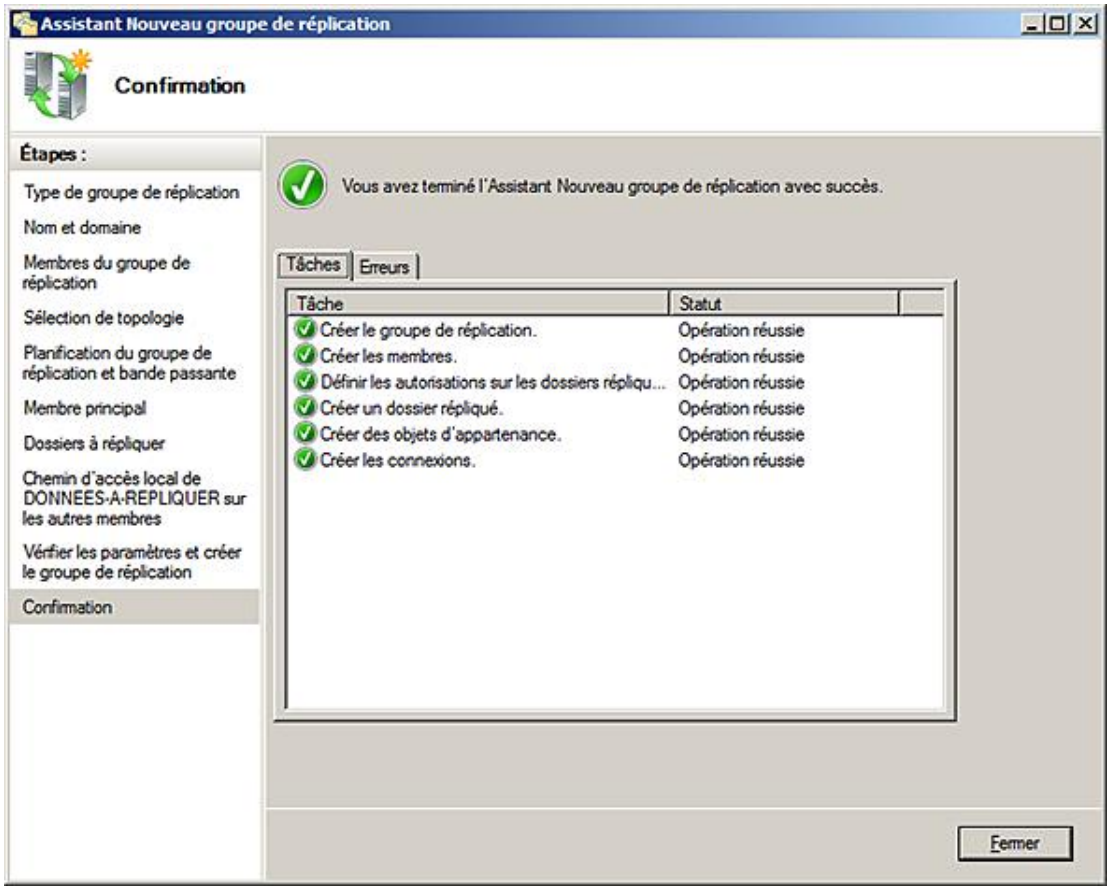

Assistant Nouveau groupe de réplication
Chemin d'accès local de DONNEES-A-REPLIQUER sur les autres membres
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Chemin d'accès local de DONNEES-A-REPLIQUER sur les autres membres
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Cliquez sur Modifier pour entrer le chemin d'accès local où stocker le dossier répliqué sur les autres membres du groupe de réplication.
Membre principal : SRVDFS
Chemin d'accès local du membre principal : C:\DONNEES-A-REPLIQUER
Détails du membre :
Membre
Chemin d'accès local
W2K8FR
C:\REPLICA-DONNEES
Modifier...
< Précédent
Suivant >
Annuler

Cet écran résume les paramètres principaux de la réplication.

© ENI Editions - All rigths reserved


Assistant Nouveau groupe de réplication
Vérifier les paramètres et créer le groupe de réplication
Étapes :
Type de groupe de réplication
Nom et domaine
Membres du groupe de réplication
Sélection de topologie
Planification du groupe de réplication et bande passante
Membre principal
Dossiers à répliquer
Chemin d'accès local de DONNEES-A-REPLIQUER sur les autres membres
Vérifier les paramètres et créer le groupe de réplication
Confirmation
Vous avez sélectionné les paramètres suivants pour le nouveau groupe de réplication. Si les paramètres sont corrects, cliquez sur Créer pour créer le groupe de réplication. Pour changer un paramètre, cliquez sur Précédent ou sélectionnez la page appropriée dans le volet d'orientation.
Paramètres du groupe de réplication :
Nom du groupe de réplication :
REPLIQUE DONNEES DOMAINE
Description du groupe de réplication :
Domaine du groupe de réplication :
MaSociete.Local
Membres du groupe de réplication (2) :
SRVDFS
W2K8FR
Type de topologie :
Maille pleine
Liste des connexions (2) :
W2K8FR -> SRVDFS
SRVDFS -> W2K8FR
Planification de connexion par défaut :
Répliquer en continu avec la bande passante Complète
< Précédent
Créer
Annuler

Voici le résultat de la mise en place de la réplication.



La mise en place effective dépendra du fonctionnement de l'Active Directory et des plannings de réplication mis en place entre les sites.

© ENI Editions - All rigths reserved

Délai de réplication
La réplication ne commencera pas tant que la configuration n'est pas recueillie par les membres du groupe de réplication. Le temps nécessaire à cette opération dépend de la latence de réplication des services de domaine Active Directory ainsi que de la fréquence d'interrogation.
Ne plus afficher ce message
OK

c. La topologie de réplication

Deux types de topologie sont proposés par défaut.

- Le mode **Hub&Spoke** dit **en étoile** nécessite trois membres au minimum. Ce mode est particulièrement utile lorsqu'il y a une source précise (le Hub) et la réplication vers de très nombreuses destinations.

- Le mode **maille pleine** autorise chaque serveur à répliquer avec les autres. Ce mode est conseillé pour les installations comportant une dizaine de membres au maximum.

La mise en place d'une nouvelle topologie dépend de la réplication Active Directory, et peut donc prendre du temps avant de se mettre en place sur chaque membre.

En revanche, la réplication locale des fichiers (de taille raisonnable) peut être très rapide, et généralement instantanée.

© ENI Editions - All rigths reserved

La configuration avancée

1. Les méthodes de classement

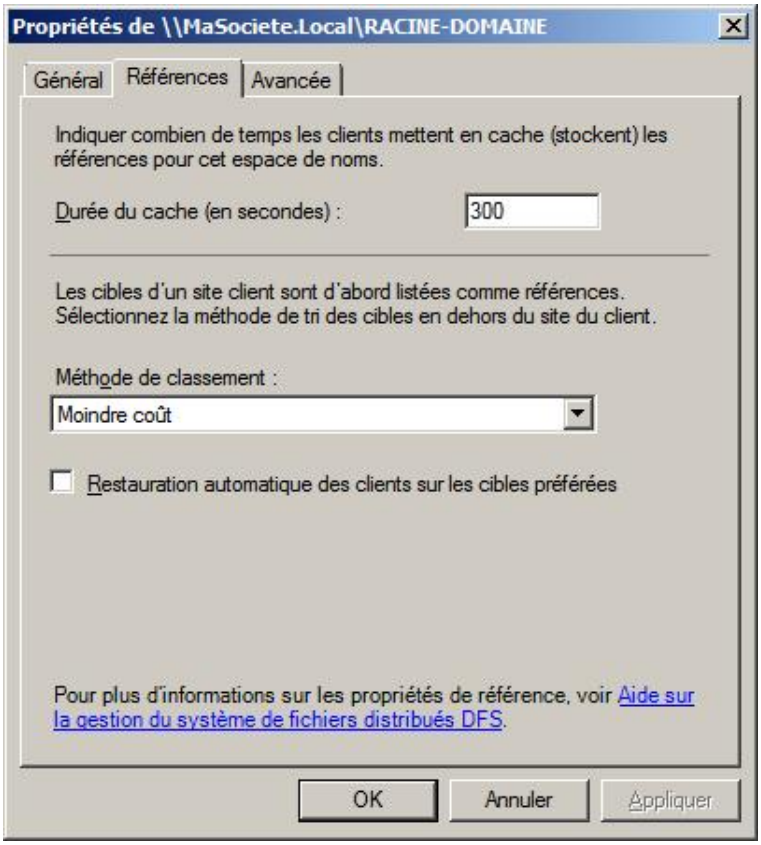
Les méthodes de classement sont très importantes à prendre en considération afin d'optimiser et d'éviter de nombreux désagréments.

En effet, lorsqu'un même dossier est accessible sur différents partages, situés sur différents serveurs, eux-mêmes situés sur des sites différents, l'optimisation logique serait d'utiliser le partage situé sur le serveur du site local. Même dans ce cas, il est parfois vital d'utiliser en priorité un serveur précis qui sert de référence. Dans d'autres cas, c'est un serveur distant qui sert de référence unique qu'il faut forcer afin d'éviter les modifications simultanées d'un document.

a. La configuration au niveau des racines DFS

L'onglet **Références** sur les propriétés des racines DFS permet de régler la valeur par défaut utilisée sur toutes les liaisons appartenant à cette racine.

- L'ordre aléatoire
- Moindre coût
- Exclusion de tous les sites distants


Propriétés de \\MaSociete.Local\RACINE-DOMAINE
Général
Références
Avancée
Indiquer combien de temps les clients mettent en cache (stockent) les références pour cet espace de noms.
Durée du cache (en secondes) :
300
Les cibles d'un site client sont d'abord listées comme références. Sélectionnez la méthode de tri des cibles en dehors du site du client.
Méthode de classement :
Moindre coût
Restauration automatique des clients sur les cibles préférées
Pour plus d'informations sur les propriétés de référence, voir Aide sur la gestion du système de fichiers distribués DFS.
OK
Annuler
Appliquer

L'**Ordre aléatoire** consiste à proposer de manière aléatoire tous les serveurs situés sur le site du client, puis toujours de manière aléatoire tous les autres serveurs présents sur les autres sites sans tenir compte des différences de coûts.

Le **Moindre coût** présentera d'abord les serveurs situés sur le site du client de manière aléatoire. Ensuite, l'affichage des serveurs distants sera proposé du coût le moins élevé au plus élevé, mais les serveurs ayant un coût identique seront proposés aléatoirement.

Le dernier mode **Exclure les cibles en dehors du site du client** n'affichera que les serveurs présents sur le site du client. Vous verrez plus loin les exceptions à cette règle.

© ENI Editions - All rigths reserved

Si la restauration automatique des clients sur les cibles préférées est forcée à ce niveau, elle sera active sur toutes les liaisons et cibles qui dépendront de cette racine.

b. La configuration au niveau des liaisons DFS

Sur chaque dossier représentant une liaison vers une ou plusieurs cibles, il est possible d'indiquer une exclusion des sites distants, notamment si celle-ci n'a pas été indiquée précédemment. On peut aussi activer la restauration automatique des clients vers une cible préférée (si celle-ci n'avait pas déjà été configurée au niveau supérieur).

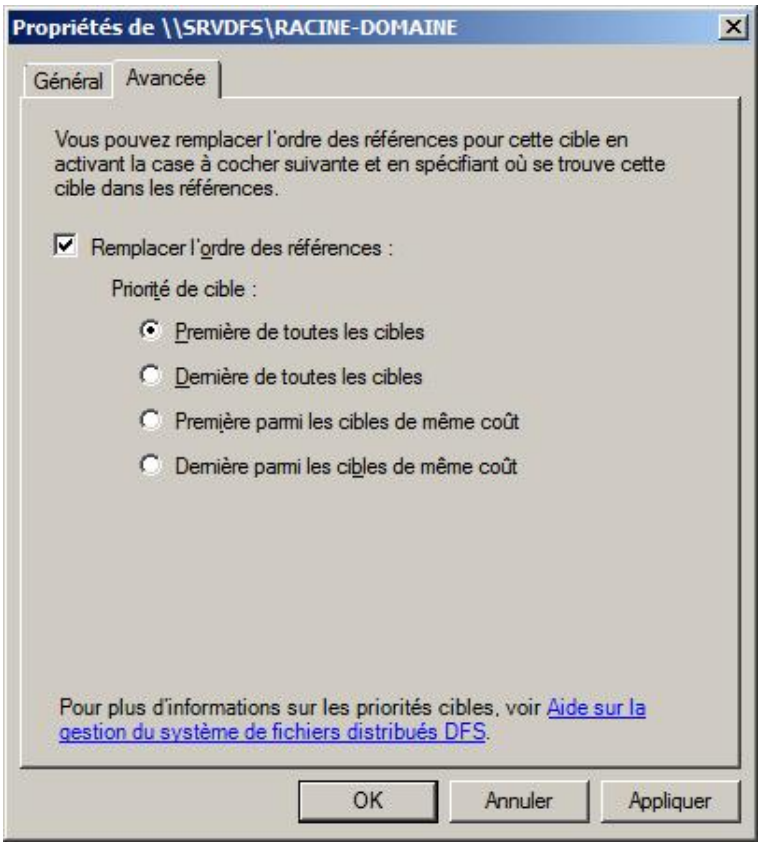
c. La configuration au niveau des cibles DFS

Sur chaque cible, dans l'onglet **Avancée**, il est possible de configurer un comportement particulier.

Il est possible de privilégier l'utilisation d'une cible en la définissant comme **Première de toutes les cibles** ou **Première de toutes les cibles de même coût**.

On peut au contraire, définir la cible comme **Dernière de toutes les cibles** affichées lors de la sélection, ou **Dernière parmi les cibles de même coût**.

Attention, ces règles forcées (Première ou Dernière) provoquent l'affichage systématique des cibles correspondantes.


Propriétés de \\SRVDFS\RACINE-DOMAINE
Général
Avancée
Vous pouvez remplacer l'ordre des références pour cette cible en activant la case à cocher suivante et en spécifiant où se trouve cette cible dans les références.
Remplacer l'ordre des références :
Priorité de cible :
Première de toutes les cibles
Dernière de toutes les cibles
Première parmi les cibles de même coût
Dernière parmi les cibles de même coût
Pour plus d'informations sur les priorités cibles, voir Aide sur la gestion du système de fichiers distribués DFS.
OK
Annuler
Appliquer

2. La délégation d'administration

Par défaut, seuls les administrateurs locaux ou du domaine peuvent gérer les groupes de réplication. Sur une racine du domaine, seul le groupe **administrateurs de l'entreprise** hérite automatiquement des droits d'administration. Sur une racine autonome, le groupe **administrateurs** local et le compte spécial **SYSTEM** ont les droits hérités.

Lorsqu'une racine est créée par un administrateur, celui-ci et le groupe **administrateurs du domaine** obtiennent des droits qui sont dit **explicites**. Ce qui veut dire que ces droits peuvent être supprimés.

Attention, les administrateurs qui ont reçu une délégation restent propriétaires des objets, même s'ils sont retirés par la suite des administrateurs.

© ENI Editions - All rigths reserved

Par ailleurs, tout administrateur d’une racine DFS peut déléguer l’autorisation de gestion.

© ENI Editions - All rigths reserved

Les apports de Windows 2008

Attention, la plupart des fonctionnalités de Windows 2008 ne sont utilisables que si les racines DFS sont gérées par des serveurs Windows 2008 dans un domaine possédant la fonctionnalité Windows 2008.

Le mode **Access-based enumeration** permet de ne montrer à l'utilisateur que les dossiers et documents sur lesquels il possède des droits. Si ce mode est bien actif par défaut sur les partages hébergés sur Windows 2008, il est nécessaire de l'activer sur les racines qui remplissent les conditions indiquées.

Voici la commande utilisant DFSUTIL permettant d'activer ce mode.

```
dfsutil property abde enable \\<namespace_root>
```

Les autres fonctionnalités propres à Windows 2008 sont :

- La recherche directe d'un dossier ou une cible DFS à partir de l'administration DFS.
- La création des racines autonomes DFS sur la machine virtuelle d'un cluster.
- La création de racines de domaine en mode **Windows Server 2008 mode domain-based namespaces** permet d'activer immédiatement les nouvelles fonctionnalités, sans avoir à convertir les anciennes racines dites en mode **domain-based namespace (Windows 2000 Server mode)**.
- La reprise accélérée de la réplication en cas de crash inattendu.
- Une sécurité particulière garantit la fraicheur du contenu en empêchant un vieux serveur de réécrire au dessus de données récentes.
- Un mécanisme de réplication amélioré aussi bien pour la réplication initiale que pour le différentiel, pour les petits et les gros fichiers.

© ENI Editions - All rigths reserved

Les outils

L'administration graphique classique permet de gérer les opérations normales et ponctuelles. Mais, de nombreuses raisons font qu'il est souvent nécessaire d'automatiser toutes ces opérations pour l'installation, la réparation ou la gestion d'environnements complexes et structurés.

Les outils en ligne de commande sont alors bien pratiques pour réaliser ce type d'opération.

Tous ces outils sont installés et utilisables directement sur tous les serveurs disposant du rôle DFS.

1. DFSCMD

La commande DFSCMD permet de gérer toute la partie **Espace de noms**, c'est-à-dire de créer et configurer une arborescence DFS.

Il n'est pas utile de reprendre toute la documentation de cette commande qui est facilement accessible.

Voici un exemple de commande qui permet de créer un batch de **réinstallation** :

```
dfscmd /view \\MaSociete.local\racine-domaine /batchrestore
```

Exemple de résultat :

```
REM BATCH RESTORE SCRIPT
REM dfscmd /map "\\MASOCIETE\RACINE-DOMAINE" "\\SRVDFS\RACINE-DOMAINE" ""
/restore
REM dfscmd /add "\\MASOCIETE\RACINE-DOMAINE" "\\W2K8FR\RACINE-DOMAINE" /restore
dfscmd /map "\\MASOCIETE\RACINE-DOMAINE\COMPTA" "\\SRVDFS\COMPTA1" "" /restore
dfscmd /add "\\MASOCIETE\RACINE-DOMAINE\COMPTA" "\\W2K8FR\compta2" /restore
```

On y retrouve les commandes de bases qui permettent de créer une racine, puis d'y ajouter des liaisons DFS.

Pour gérer la partie réplication, il sera nécessaire d'utiliser la commande `DFSRADMIN` !

2. DFSRADMIN

L'outil permet de créer/supprimer/lister les éléments de la réplication DFS.

La commande suivante permet de générer un rapport de la réplication du dossier choisi :

```
DFSRADMIN PROPREP NEW /RgName :GroupeReplication
/RfName :DossierRépliqué /MemName :Domaine\Serveur
```

Comme la commande DFSCMD, elle permet d'automatiser la création d'ensembles de réplication à partir d'un fichier grâce à l'option **Bulk**.

3. DFSRDIAG

Cette commande permet de vérifier le bon fonctionnement, de diagnostiquer et de gérer l'activité de la réplication.

Il est possible de forcer une réplication sur une connexion précise, ou au contraire de l'arrêter immédiatement.

4. DFSUTIL

Cette commande permet de gérer les espaces de noms, les serveurs et les clients DFS.

5. DFSRMIG

Cet utilitaire ne sert pas dans l'utilisation normale de DFS. Il s'agit plutôt d'un outil d'optimisation de la réplication des

© ENI Editions - All rigths reserved

fichiers utilisés par AD.

La commande `DFSRMIG` permet en effet de migrer la réplication de SYSVOL du mode **NTFRS (Réplication 2003)** vers le mode **DFSR (Réplication 2008)**.

Elle permet aussi de vérifier le statut de cette migration sur les différents contrôleurs de domaine.

Certaines options particulières ne seront utiles que dans l'administration des contrôleurs de domaine en lecture uniquement (RODC) lors de leur migration en mode DFSR.

Vous trouverez plus d'informations sur les RODC dans le chapitre Domaine Active Directory de ce même ouvrage.

© ENI Editions - All rigths reserved

L’utilisation et les bons usages

L’utilisation de DFS ne nécessite aucune adaptation sur les postes clients.

En effet, côté utilisateur (et des clients Windows), les partages DFS et les racines sont vus comme des partages classiques. C’est souvent dans le script de connexion que l’on réalise la connexion aux racines, souvent en remplacement de toutes les anciennes connexions.

Par ailleurs, il est important de noter que les racines DFS de domaine sont disponibles pour tous les utilisateurs de la forêt. Mais, toutes les permissions affectées aux partages et aux dossiers NTFS restent totalement actives comme s’il s’agissait d’un accès direct.

En revanche, l’utilisation de DFS permet de simplifier le nombre d’unités disques et de partages utilisés. Ceci permet de fédérer l’ensemble des espaces disponibles.

Les applications peuvent être configurées sur un chemin unique qu’il sera possible de maintenir durant toute la vie de la forêt.

DFS dans la configuration **Hub&Spoke** est préconisé pour la réplication sur de nombreux sites d’informations bougeant peu ou n’ayant qu’un seul point de modification. Les procédures validées, notices, comptes-rendus et informations générales sont les documents entrant dans ce type de configuration.

DFS peut aussi être utilisé pour sauvegarder les données utilisateurs ou les profils itinérants. Une configuration particulière doit alors être réalisée au niveau des cibles DFS afin que ce soit toujours le même partage et le même serveur qui soient utilisés. C’est-à-dire, de toujours proposer la cible principale en premier, et de ne proposer la copie (sauvegarde) qu’en dernière cible.

Lorsque DFS est utilisé pour la bureautique, avec de nombreux documents de type Word ou Excel, mis à jour sur différents site, il est important de bien gérer le versionning des documents afin d’éviter toute modification « simultanée » d’un même document. En effet, seule la dernière version écrite sera conservée. Dans certains cas, il sera préférable de forcer l’utilisation d’une cible précise qui servira de référence pour les modifications de ce genre, même si le site de l’utilisateur comporte la réplication locale de cette cible.

Donc, DFS n’est pas la solution universelle, mais elle peut rendre de nombreux services qu’il faut comparer aux autres solutions, par exemple de gestion documentaire.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre présente les deux systèmes de messagerie prévus pour s'installer sur Windows 2008 : le système SMTP intégré à Windows 2008 et la messagerie Exchange 2007 SP1 dont les différentes contraintes d'installation seront examinées.

© ENI Editions - All rigths reserved

La mise en place d'un système de messagerie SMTP

La définition de **SMTP** (*Simple Mail Transfer Protocol*) ne correspond au départ qu'à un protocole **normalisé** utilisé entre deux machines pour se transférer un message. Par extension, on sous-entend dans **Messagerie SMTP** tous les mécanismes (service, queues…) servant à sa mise en œuvre.

Attention donc à cette appellation tendancieuse, un système de messagerie **SMTP** à lui seul ne constitue pas ainsi un système de messagerie. De la même manière, SendMail et Postfix ne font qu'une partie du travail, c'est-à-dire déplacer les messages entre différents serveurs de messagerie. Vu de l'utilisateur, SMTP ne permet à l'utilisateur que de déposer des messages dans le circuit de distribution.

Il manque donc dans ces systèmes la partie essentielle qui intéresse l'utilisateur, c'est-à-dire l'accès, la récupération et la lecture des messages proprement dits. Cette fonctionnalité de base qui était fournie dans Windows 2003 sous la forme d'un service **POP3** n'existe plus dans Windows 2008. Les utilisateurs de ce type de solution devront conserver un serveur Windows 2003 ou adopter une autre messagerie ! Il est vrai que la législation européenne et internationale qui impose régulièrement des normes d'archivage et de conservation supplémentaires rend ce système peu efficace et peu adapté.

À quoi sert donc ce service SMTP ?

SMTP sert tout d'abord à faire ce pourquoi il a été conçu, c'est-à-dire de plaque tournante d'un **MTS** (*Messaging Transfer System*). Les messages sont reçus, classés dans des queues en fonction des domaines d'expédition, mis en attente si nécessaire, puis dispatchés ou retransmis en fonction de critères choisis.

On retrouve donc souvent les services SMTP en contact direct avec Internet, notamment dans des DMZ, pour soulager les serveurs de messagerie lorsque le traitement des messages entrants et sortants devient significatif. Tout le travail de résolution DNS, de communication avec les serveurs distants et de remise du contenu est ainsi déporté sur une machine (ou plusieurs) différente.

Ce point névralgique devient un endroit de choix pour installer des solutions de filtrages ANTISPAM et antivirus. Dans d'autres cas, il peut servir de serveur de secours pour continuer à recevoir les messages lorsque le serveur de messagerie traditionnel n'est pas accessible (arrêt, sauvegarde…).

Pour les sociétés ou logiciels (SAP, Sharepoint, etc.), qui peuvent émettre de grosses quantités de messages pas forcément destinés à la messagerie locale, l'utilisation directe d'un système SMTP permettra d'éviter le passage à travers la messagerie de l'entreprise, et d'obtenir un traitement beaucoup plus rapide des envois.

1. Mise en place d'un système SMTP

Windows est segmenté en rôles principaux et fonctionnalités indépendantes.

Le service SMTP est une des 35 **fonctionnalités** proposées.

a. L'installation

L'installation de ce service peut se faire très simplement par la commande suivante :

```
Servermanagercmd -install SMTP-Server
```

Ce modèle implique l'installation de l'administration **IIS** et du mode compatible **IIS6**. L'administration de ce service se retrouve donc logiquement dans la console d'administration des services IIS6.

b. La configuration

Lors de l'installation initiale, un premier serveur virtuel SMTP est créé automatiquement. Ce premier serveur virtuel utilise la valeur standard 25 du protocole SMTP en entrée et en sortie. Il est possible de créer d'autres serveurs virtuels SMTP pour des besoins de communications spécifiques, sécurisés ou non, mais définis sur des ports différents.

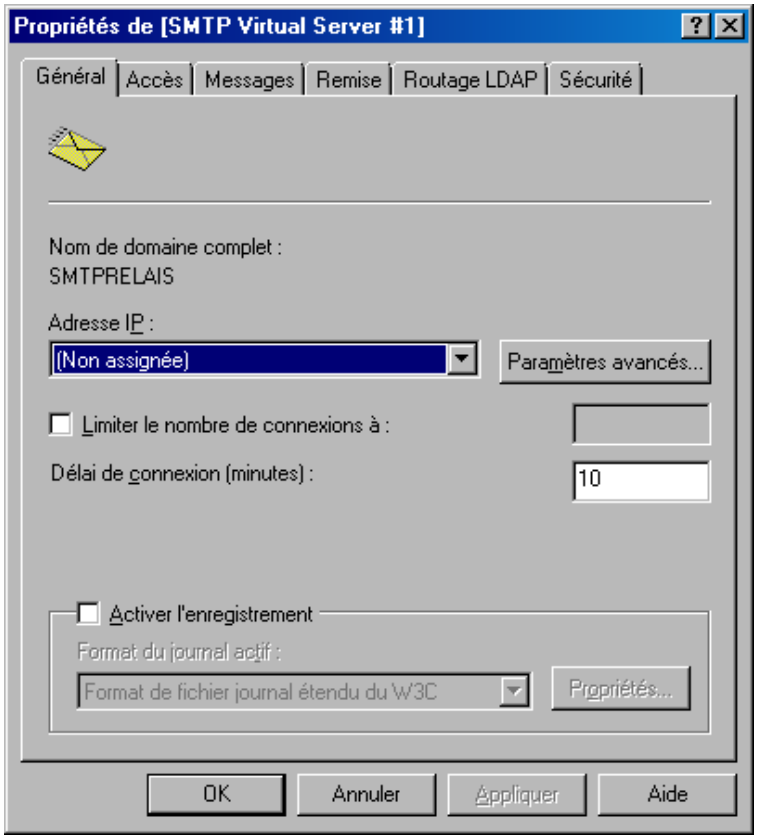
Le serveur virtuel par défaut est configuré de base pour autoriser les connexions anonymes en entrée, mais il n'autorise pas le relais des messages sauf pour les ordinateurs authentifiés. Il ne peut donc pas servir de serveur relais aux spammeurs. L'envoi des messages se fait aussi en mode anonyme. Si ce serveur doit communiquer directement avec toutes les autres messageries sur Internet, le mode **anonyme** est normal et impératif.

Pour fonctionner correctement, le serveur doit pouvoir rechercher les adresses IP des serveurs distants par DNS, et être autorisé par les systèmes de protection en place à utiliser le port SMTP (25) en sortie et en entrée.

Attention, toute modification de la configuration par défaut a une incidence !

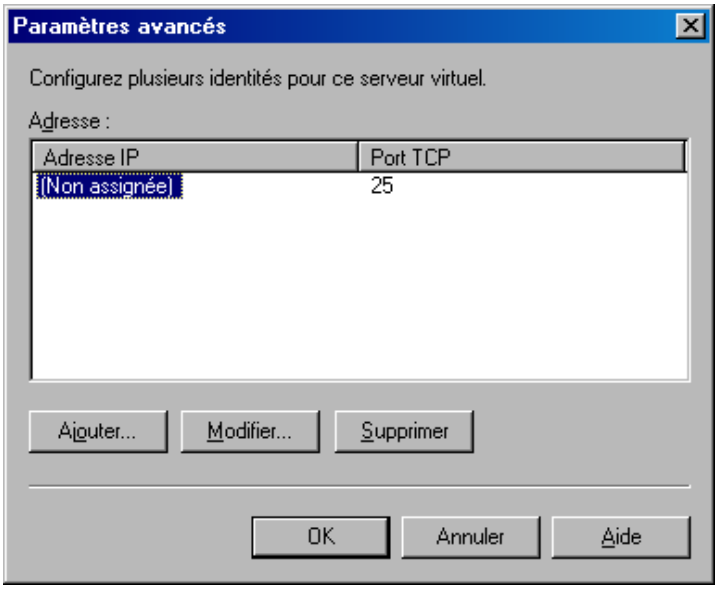
© ENI Editions - All rigths reserved

L'onglet **Général** permet d'accéder à deux points de configuration importants :



L'activation de l'enregistrement des logs est à réaliser dès que des problèmes ou des doutes apparaissent sur la communication avec certains serveurs distants.

En cliquant sur le bouton **Paramètres avancés**, il est possible de modifier les ports et les cartes utilisés.



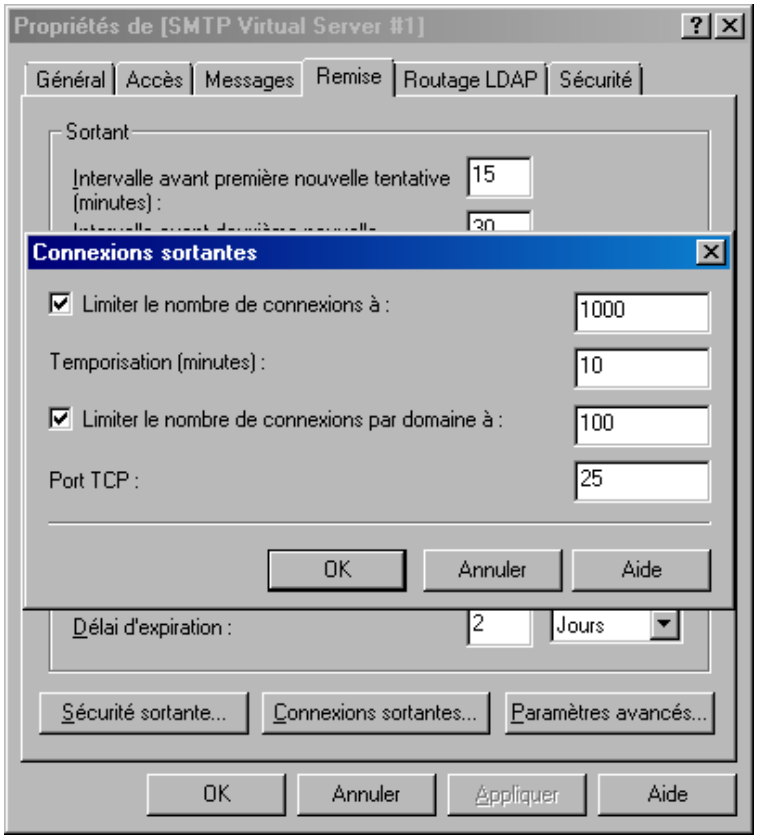
L'onglet **Accès** permet de définir quels sont les systèmes autorisés à déposer des messages. En revanche, seuls les systèmes authentifiés ou autorisés pourront utiliser la fonction de relais. C'est-à-dire de déposer un message destiné à des domaines différents des domaines locaux. Habituellement, seuls les serveurs de messagerie internes à l'entreprise devraient apparaître à ce niveau.

Les paramètres principaux des onglets **Messages** et **Remise** sont assez clairs naturellement. En revanche, la configuration avancée de la remise n'est pas toujours évidente. La sécurité sortante permet d'activer le chiffrement, et l'authentification sur un compte précis lorsque le serveur virtuel a pour but de se connecter sur des serveurs particuliers.

Les connexions sortantes permettent principalement de modifier le port de communication utilisé pour interroger les

© ENI Editions - All rigths reserved

serveurs distants.



Si les différentes limites (nombre de connexions, durées…) conviennent à la plupart des clients, il faut parfois les adapter à la situation.

Par exemple, si tous les messages passent par un autre relais SMTP, il est inutile de limiter les connexions par domaine. Sur les sites importants, la limite du nombre de connexions doit souvent être retirée, et la temporisation, c'est-à-dire le temps que la connexion est maintenue après le dernier message, diminuée.

Après modification de ces paramètres, il faut redémarrer le service SMTP ou le serveur virtuel pour une prise en compte des modifications.

Attention, l'arrêt du service SMTP provoque l'arrêt de tous les serveurs virtuels.

Utilisez la ligne de commande suivante :

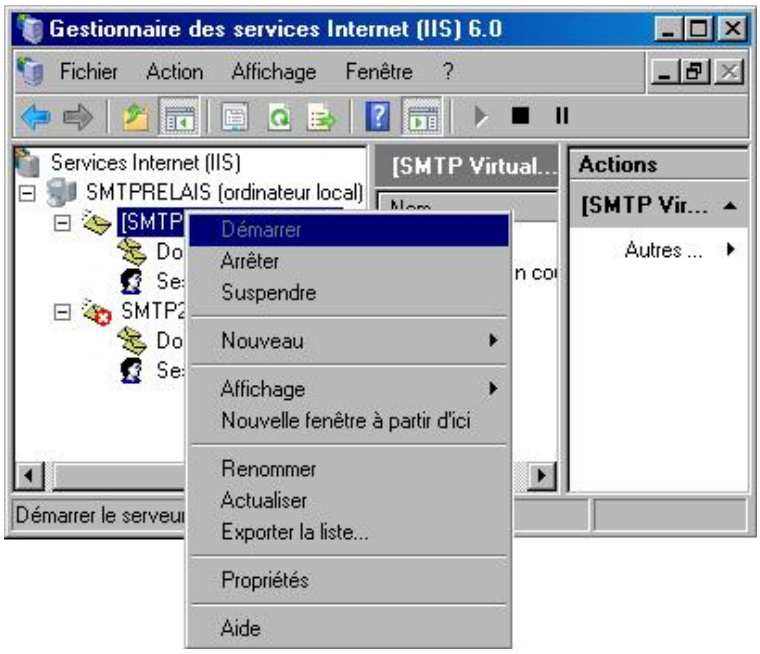
```
NET STOP SMTPSVC
```

Puis

```
NET START SMTPSVC
```

En revanche, les serveurs virtuels SMTP peuvent être arrêtés séparément dans l'interface graphique soit en passant par le menu contextuel (clic droit sur le serveur virtuel), soit en utilisant la barre d'outils qui contient les symboles classiques d'arrêt et de démarrage.

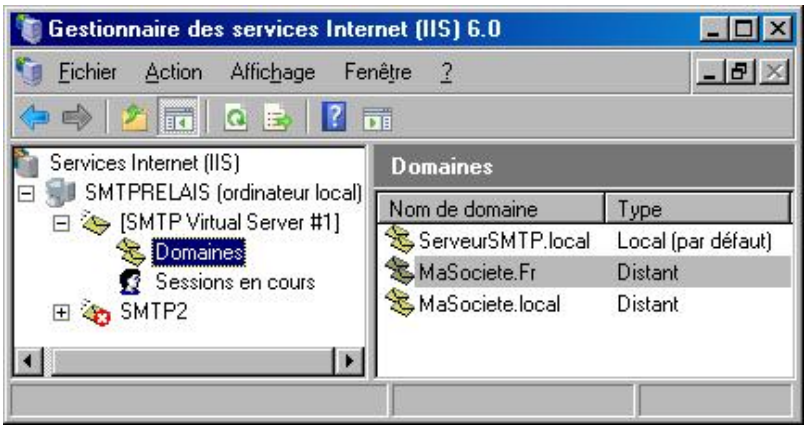
© ENI Editions - All rigths reserved



c. L'utilisation

Une fois que la configuration de base est réalisée, l'utilisation principale est d'autoriser et de rediriger le ou les domaines de messagerie de l'entreprise vers les serveurs gérant effectivement ces domaines.

Le conteneur **Domaines** permet de définir tous les domaines de messagerie acceptés et connus par ce serveur SMTP.

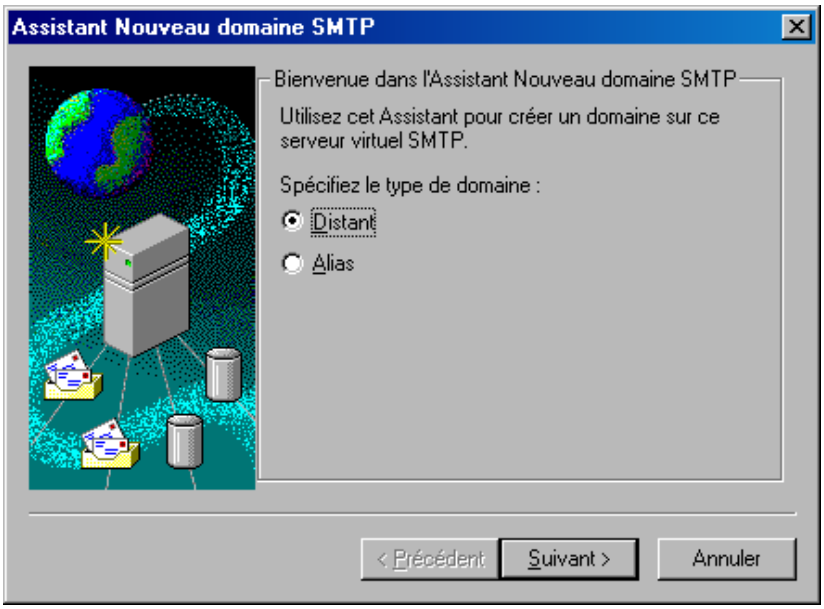


On peut dire qu'un système de messagerie SMTP est en place dès qu'il sait envoyer des messages vers Internet et qu'au moins un domaine de messagerie interne est défini.

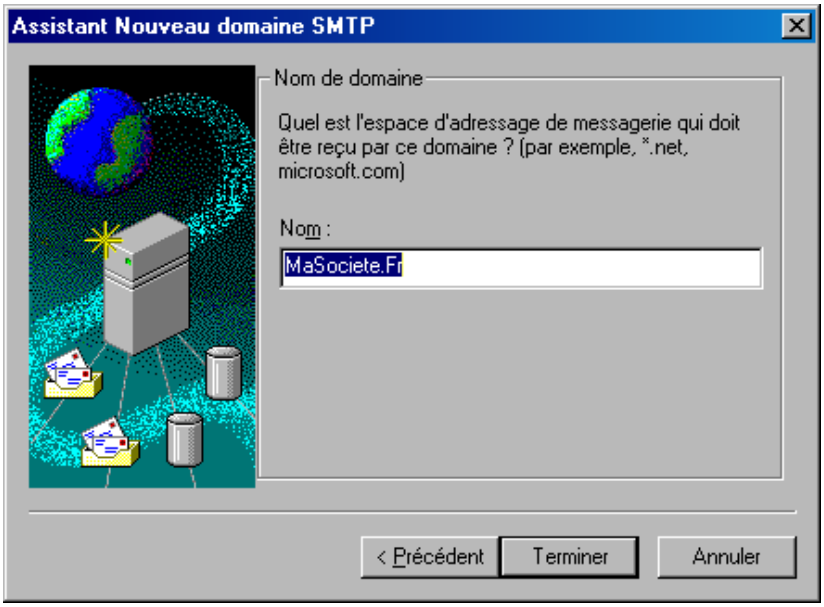
À noter que le domaine de type local correspond à un système de messagerie par défaut associé à la machine elle-même, lui permettant de recevoir des messages spécifiques qui lui sont destinés et qui seront mémorisés (en vrac) dans un dossier. Son utilisation réelle est assez rare, et suppose un logiciel pour traiter ces messages.

- Cliquez avec le bouton droit de la souris sur **Domaines** puis choisissez **Nouveau**. Pour tout domaine qui n'est pas géré par le serveur SMTP localement, choisissez **Distant**.

© ENI Editions - All rigths reserved


Assistant Nouveau domaine SMTP
Bienvenue dans l'Assistant Nouveau domaine SMTP
Utilisez cet Assistant pour créer un domaine sur ce serveur virtuel SMTP.
Spécifiez le type de domaine :
Distant
Alias
< Précédent
Suivant >
Annuler

- Indiquez le domaine géré de manière spécifique.

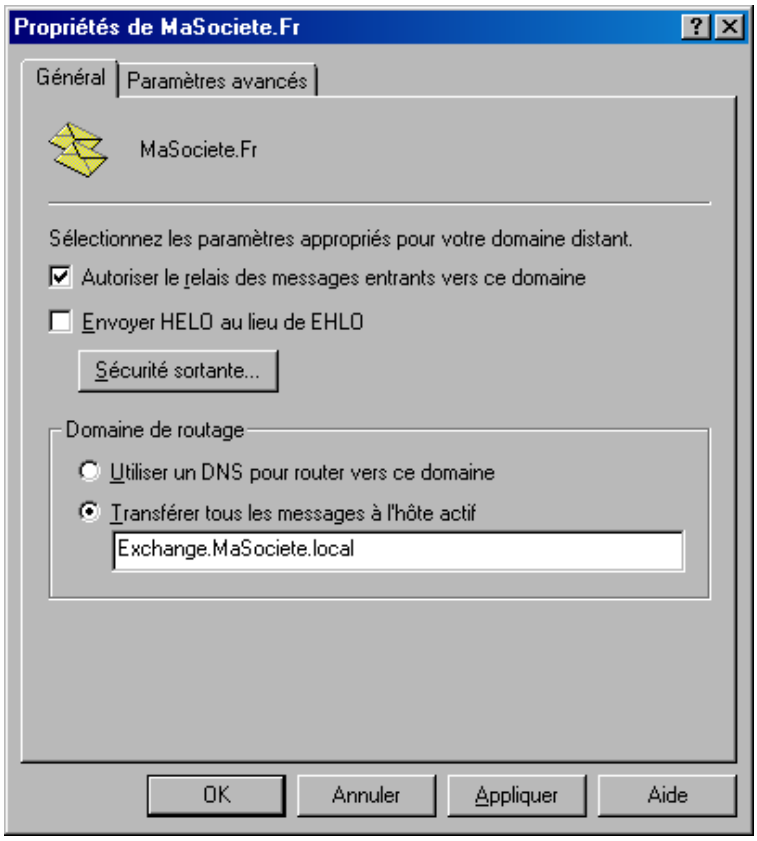

Assistant Nouveau domaine SMTP
Nom de domaine
Quel est l'espace d'adressage de messagerie qui doit être reçu par ce domaine ? (par exemple, *.net, microsoft.com)
Nom :
MaSociete.Fr
< Précédent
Terminer
Annuler

À ce niveau, il est important d'indiquer le domaine de messagerie qui est effectivement référencé sur Internet.

Un nom DNS est obligatoire pour la redirection basée sur la résolution DNS. S'il n'est pas possible d'obtenir la résolution DNS correcte sur le réseau interne, la solution est de définir les noms des serveurs nécessaires dans le fichier HOSTS.

Pour indiquer le nom du serveur de destination, double cliquez sur le domaine pour atteindre l'écran suivant. Au lieu d'utiliser la résolution DNS classique qui provoquerait probablement une boucle, utilisez l'option **Transférer tous les messages à l'hôte actif** pour définir soit une adresse IP entre crochets, soit encore mieux une adresse DNS complète correspondant au réseau local (à ajouter dans le fichier HOSTS).

© ENI Editions - All rigths reserved



d. Les tests et vérifications

Pour réaliser les tests de bases, l'outil de test principal est tout simplement **Telnet.exe**.
Par étape progressive, on pourra tester le fonctionnement :

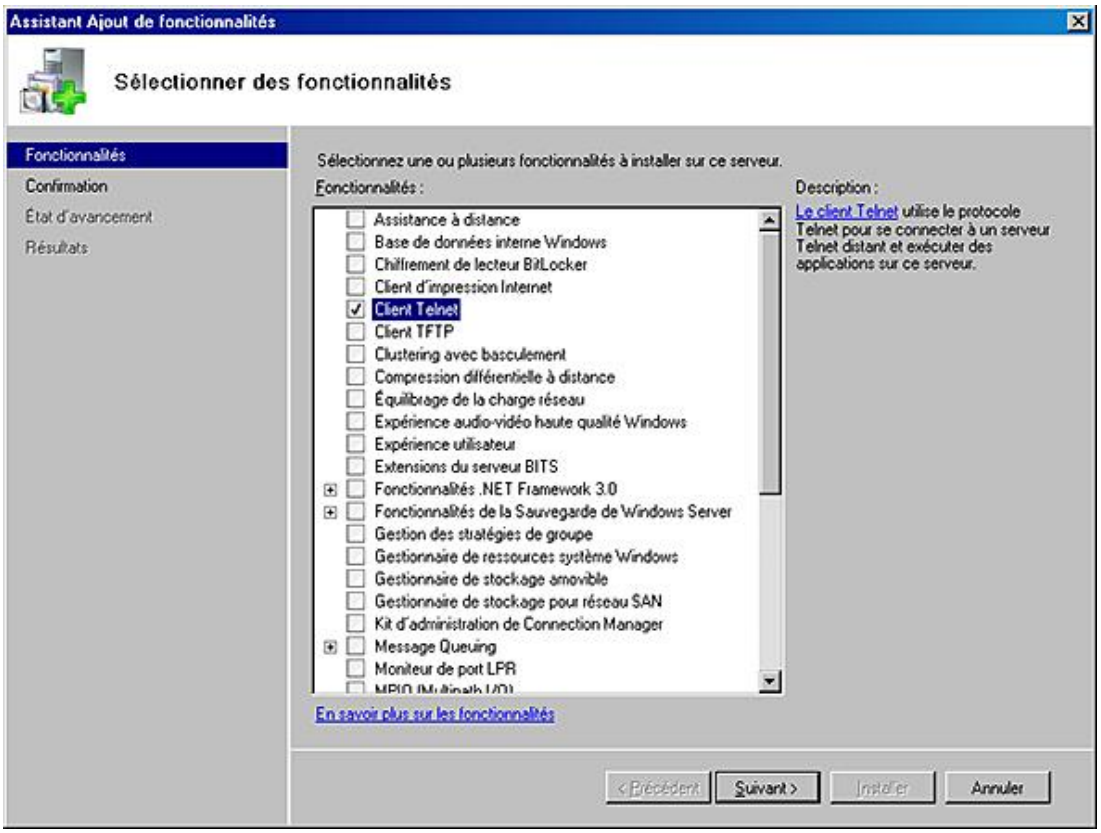
- sur le serveur lui-même ;
- sur une machine du réseau ;
- depuis une machine connectée depuis Internet.

La commande `telnet NomDuServer.domaine.Extension 25` permet de tester deux points précis :

- la résolution DNS de la machine ;
- l'autorisation effective du protocole 25.

Le **client telnet** est une fonctionnalité de Windows 2008 qu'il faut installer :

© ENI Editions - All rigths reserved


Assistant Ajout de fonctionnalités
Sélectionner des fonctionnalités
Fonctionnalités
Confirmation
État d'avancement
Résultats
Sélectionnez une ou plusieurs fonctionnalités à installer sur ce serveur.
Fonctionnalités :
Assistance à distance
Base de données interne Windows
Chiffrement de lecteur BitLocker
Client d'impression Internet
Client Telnet
Client TFTP
Clustering avec basculement
Compression différentielle à distance
Équilibrage de la charge réseau
Expérience audio-vidéo haute qualité Windows
Expérience utilisateur
Extensions du serveur BITS
Fonctionnalités .NET Framework 3.0
Fonctionnalités de la Sauvegarde de Windows Server
Gestion des stratégies de groupe
Gestionnaire de ressources système Windows
Gestionnaire de stockage amovible
Gestionnaire de stockage pour réseau SAN
Kit d'administration de Connection Manager
Message Queuing
Moniteur de port LPR
Description :
Le client Telnet utilise le protocole Telnet pour se connecter à un serveur Telnet distant et exécuter des applications sur ce serveur.
En savoir plus sur les fonctionnalités
< Précédent
Suivant >
Installer
Annuler

Si l'affichage de la ligne commence par **220 SMTP….** , alors la configuration de base est correcte.

Sinon, vérifiez la résolution DNS avec ping :

```
Ping NomDuServeur.Domaine.Extension
Ping Adresse IP
```

Puis telnet avec l'adresse IP :

```
Telnet AdresseIP 25
```

Dès que ces tests fonctionnent, y compris depuis Internet, on peut maintenant passer à l'étape suivante qui consiste à vérifier la possibilité d'envoyer des messages, de relayer ou non vers certains domaines si cela a été autorisé.

Se connecter au serveur :

```
Telnet AdresseIP 25
```

Réaliser un envoi classique :

```
HELO test
MAIL FROM : VotreAdresse@VotreDomaine.Extension
RCPT TO: ping@oleane.net
DATA
Test.
.
QUIT
```

Attention, lors de la saisie des commandes, aucune erreur n'est autorisée. Si vous utilisez la touche de retour en arrière, il vous faudra ressaisir totalement la ligne correspondante.

Pour tester le relais, il suffira de remplacer votre adresse de messagerie par une adresse externe. L'erreur 454 en réponse à la commande RCPT TO signifie que le relais est refusé.

À noter que **NsLookup** n'est pas forcément le bon outil dans un environnement classique Microsoft, car il suppose que des zones DNS sont configurées (et correctement). Or, les zones de recherches inversées ne sont pas nécessaires dans un environnement purement Microsoft. Donc, le fait que NsLookup ne vous donne pas les réponses attendues localement ne signifie pas que votre configuration soit mauvaise. En revanche, vous pourrez l'utiliser pour

© ENI Editions - All rigths reserved

les zones DNS sur Internet.

Les bonnes pratiques vous encourageront à créer et gérer les zones reverses afin de disposer de tous les éléments nécessaires, et même utiliser NsLookup !

2. Réservation d'un nom de domaine sur Internet

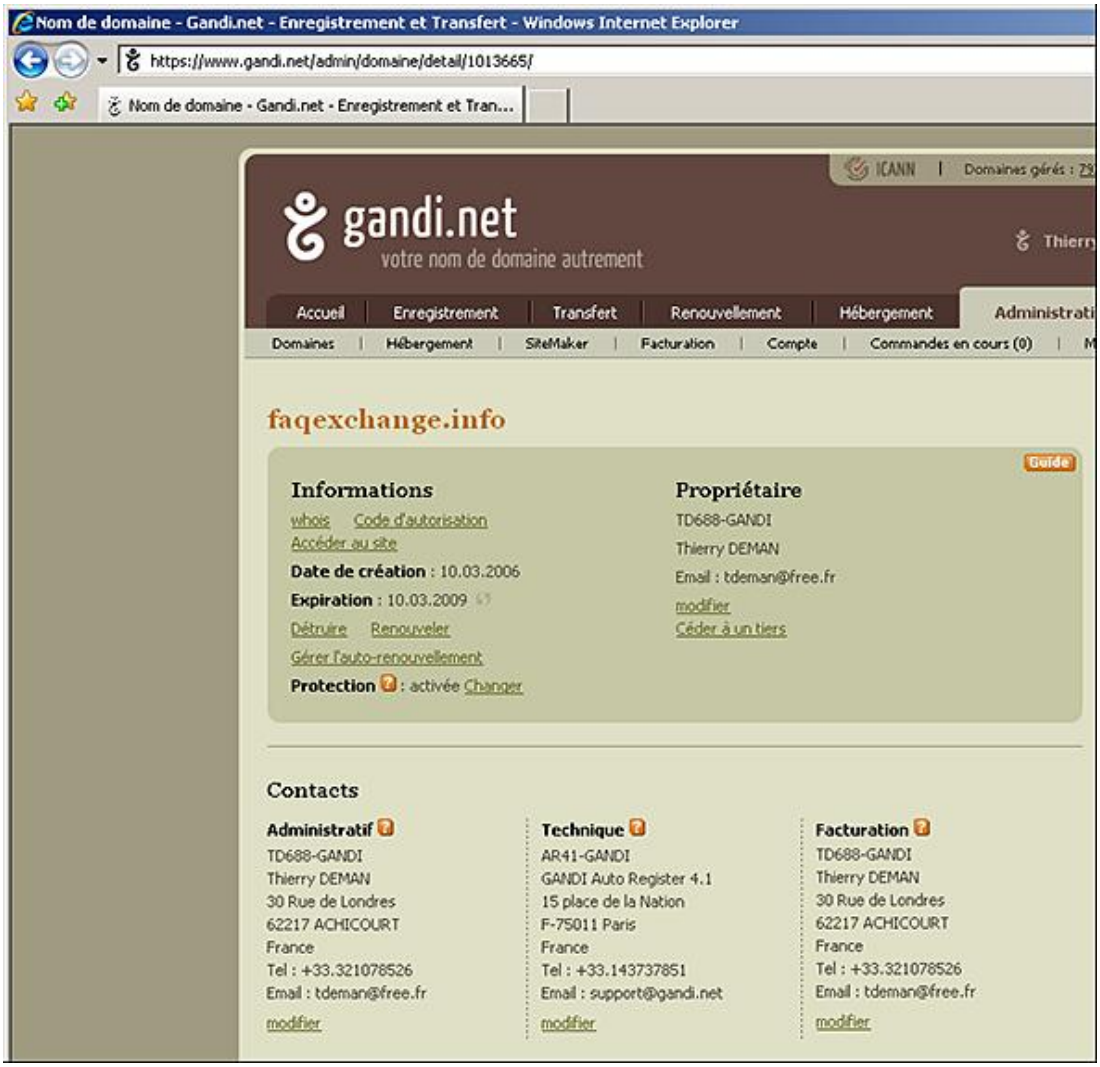
La réservation d'un nom de domaine consiste à acheter, en réalité à louer, un nom précis qui sera connu sur l'ensemble du réseau Internet. Ce nom, et tous les éléments qui en dépendent, feront partie de ce que l'on appelle une zone DNS. La personne morale qui réserve ce nom de domaine sera responsable de l'intégralité du contenu.

Généralement, deux contacts sont spécifiés lors de l'enregistrement : un responsable **administratif** et un responsable **technique**. Ces personnes seront les seules habilitées à demander les modifications du contenu de la zone.

Les noms de domaine que l'on peut utiliser dépendent de la personne morale que l'on représente. Selon l'extension choisie, les règles seront différentes et plus ou moins contraignantes. Il n'y a quasiment aucune règle pour les domaines en **.COM** ou **.INFO** où la seule date de la première demande fait foi. En revanche, obtenir une extension **.FR** suppose de fournir un extrait KBIS, une inscription INPI pour les marques, ou une preuve équivalente…

Les démarches peuvent se faire soit directement sur les sites d'enregistrements dits **registrar** qui sont chargés de gérer certaines extensions, soit par l'intermédiaire des fournisseurs d'accès Internet. Dans tous les cas, vérifiez bien que ce soit votre nom qui soit associé au domaine souhaité en tant que **propriétaire**, et non la société intermédiaire. Sinon, en cas de conflit, il sera difficile de faire valoir vos droits.

Voici un exemple d'enregistrement réalisé auprès de la Société GANDI :



3. La gestion d'un serveur DNS externe

Les zones DNS **publiques** sont très rarement gérées au sein de l'entreprise elle-même. Seules les entreprises de

© ENI Editions - All rigths reserved

grande taille prennent généralement le risque et la charge de gérer directement ces DNS.

Quand la zone publique est gérée sur Internet, l'interface d'administration du fournisseur d'accès Internet ou de l'organisme sur lequel le domaine a été acheté (Gandi, Amen, DynDns…). Chacun de ces fournisseurs possède une interface Web spécifique très souvent en anglais et des possibilités plus ou moins étendues de configuration.

La gestion d'un serveur DNS et d'une zone DNS sur Internet provoque souvent des questions sur le nom de la zone DNS qu'il faut installer et utiliser sur le réseau interne.

Lorsque le réseau local interne utilise la même zone DNS que celle définie sur Internet, ceci provoque des problèmes de résolutions et donc d'accès sur celle définie sur Internet. Ceci est le choix de Microsoft et généralement des grosses structures. Ceci suppose d'avoir en réalité deux zones DNS gérées séparément, avec une séparation forte entre les deux. Certaines mises à jour seront donc réalisées deux fois pour être vues et accédées à la fois sur Internet et en local. C'est souvent le cas pour les sites Web de l'entreprise qui sont hébergés sur Internet. Il faut créer une entrée statique dans la zone DNS interne avec l'adresse IP externe pour chacun de ces sites.

Si les domaines sont différents, la séparation entre les deux environnements sera claire, mais provoquera des petits soucis lors de la demande de certificats. Ceci peut aussi perturber l'utilisateur lors de ses accès distants. Parfois, il devra utiliser des noms composés du domaine DNS externe, et parfois du domaine interne, par exemple pour s'authentifier !

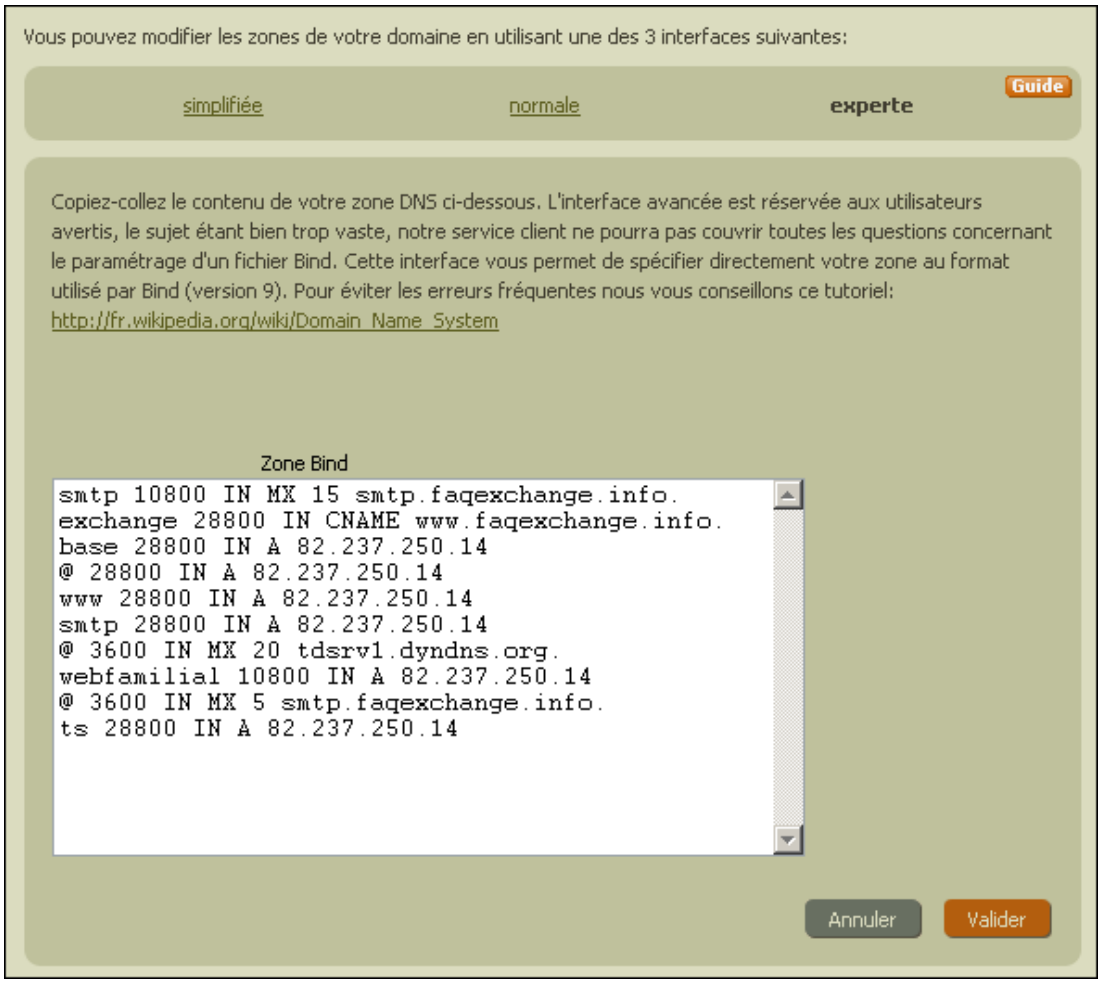
Voici un exemple d'administration en mode **normal** de DNS hébergé sur Internet :

Modification de zone DNS
Rappel: Vous travaillez actuellement sur le domaine faqexchange.info
Dans le but d'offrir un maximum de services à nos clients, nous vous proposons d'utiliser au mieux les serveurs de noms de GANDI en modifiant directement vos zones DNS.
Ce domaine est sur le fichier de zone faqexchange.info import 1, pour voir la liste des zones à votre disposition rendez-vous sur votre interface de gestion de zone.
Vous pouvez modifier les zones de votre domaine en utilisant une des 3 interfaces suivantes:
simplifiée
normale
experte
Guide
Nom Type Valeur Prio TTL
@ A 82.237.250.14 8 heures
base A 82.237.250.14 8 heures
smtp A 82.237.250.14 8 heures
ts A 82.237.250.14 8 heures
webfamilial A 82.237.250.14 3 heures
www A 82.237.250.14 8 heures
exchange CNAME www.faqexchange.info. 8 heures
@ MX tdsrv1.dyndns.org. 20 1 heure
@ MX smtp.faqexchange.info. 5 1 heure
smtp MX smtp.faqexchange.info. 15 3 heures
Retour
Ajouter un enregistrement

Pour l'administration de la partie messagerie, c'est la ligne **@ MX** qui est importante. En effet, elle correspond à la globalité du domaine de messagerie. Si plusieurs lignes de ce type existent, il existe une notion de coût qui permet d'établir la priorité d'utilisation. Le coût le plus faible (1 dans l'exemple) correspondra à la première adresse utilisée pour la remise du message.

GANDI propose aussi une interface dite experte permettant de modifier directement le texte de son fichier BIND-DNS.

© ENI Editions - All rigths reserved


Vous pouvez modifier les zones de votre domaine en utilisant une des 3 interfaces suivantes:
simplifiée
normale
experte
Guide
Copiez-collez le contenu de votre zone DNS ci-dessous. L'interface avancée est réservée aux utilisateurs avertis, le sujet étant bien trop vaste, notre service client ne pourra pas couvrir toutes les questions concernant le paramétrage d'un fichier Bind. Cette interface vous permet de spécifier directement votre zone au format utilisé par Bind (version 9). Pour éviter les erreurs fréquentes nous vous conseillons ce tutoriel:
http://fr.wikipedia.org/wiki/Domain_Name_System
Zone Bind
smtp 10800 IN MX 15 smtp.faqexchange.info.
exchange 28800 IN CNAME www.faqexchange.info.
base 28800 IN A 82.237.250.14
@ 28800 IN A 82.237.250.14
www 28800 IN A 82.237.250.14
smtp 28800 IN A 82.237.250.14
@ 3600 IN MX 20 tdsrv1.dyndns.org.
webfamilial 10800 IN A 82.237.250.14
@ 3600 IN MX 5 smtp.faqexchange.info.
ts 28800 IN A 82.237.250.14
Annuler
Valider

© ENI Editions - All rigths reserved

La mise en place d'une messagerie Exchange

Exchange 2007 SP1 est actuellement la seule version d'Exchange prévue par Microsoft pour fonctionner sur Windows 2008, et ce uniquement en version 64 bits. À noter que contrairement aux anciennes versions d'Exchange 2000 et 2003, le service SMTP ne doit surtout pas être installé, et NNTP a complètement disparu.

Le SP1 de Exchange est en réalité une version complète d'environ 1,2 Go !

Nous allons passer en revue les composants Windows 2008 nécessaires et suffisants de Windows 2008, puis pour Exchange 2007 avec les spécificités de son installation sur Windows 2008.

1. Les besoins au niveau de Windows

Les besoins de Windows 2008 sont assez classiques et sont largement dépassés par la plupart des machines actuelles.

La seule réelle restriction consiste à utiliser un processeur 64 bits et la version 64 bits de Windows 2008. Windows 2008 et Exchange 2007 utiliseront de manière optimale toute la mémoire proposée. De très bons résultats seront obtenus à partir de 4 Go, dans tous les cas, meilleurs que ceux obtenus par Exchange 2003 en 32 bits sur la même machine. En effet, Exchange 2003 32 bits ne sait pas utiliser efficacement plus de 3 Go !

Avant d'installer Exchange 2007, certains modules précis de Windows 2008 sont requis.

Contrairement aux anciennes habitudes liées aux versions antérieures de Windows, par mesure de sécurité, il est préférable de n'installer que les composants nécessaires.

Pour préparer Windows 2008, la liste des composants à installer est clairement établie en fonction des rôles du serveur Exchange.

2. Un rappel rapide des différents rôles Exchange

Il existe cinq rôles bien différenciés sur Exchange dont trois sont indispensables. Attention, certains rôles peuvent être hébergés sur un même serveur mais pas tous. Les rôles indispensables sont :

- CAS = Le frontal d'accès pour les protocoles Internet (http, Pop3, Imap).

  Le serveur CAS sert aussi de passerelle pour les accès RPC sur http !

- HUB = Transport des messages (SMTP).

- MAILBOX = Gestion des banques d'information et des boîtes.

Attention, dès que le rôle MAILBOX est configuré en cluster, il ne peut plus être combiné avec un autre rôle.

Les rôles spécifiques :

- UM = Messagerie Unifiée.

  Ce rôle sera principalement déployé pour interfacer la téléphonie (et le fax) avec la messagerie.

- EDGE = Passerelle SMTP (de filtrage).

Un serveur possédant le rôle EDGE ne devra jamais être intégré dans la forêt contenant la messagerie Exchange. Le serveur EDGE remplit la même fonction que le service SMTP présenté dans la première partie de ce chapitre, à ceci près qu'il intègre toutes les fonctionnalités de filtrage et d'antispam d'Exchange 2007. Ce rôle est totalement incompatible avec les autres rôles. À noter que le même filtrage peut aussi être activé sur le rôle HUB.

3. Les composants Windows à installer en fonction du rôle

© ENI Editions - All rigths reserved

	Contrôleur de domaine 2008	EDGE	CAS	HUB	MAILBOX	UM
Joindre le domaine		Non	Oui	Oui	Oui	Oui
Droits nécessaires	Entreprise, Schema	Locaux	Locaux+ Exchange	Locaux+ Exchange	Locaux+ Exchange	Locaux+ Exchange
Sur le DC gérant le schéma	RSAT-ADDS					
Outil nécessaire		PowerShell	PowerShell	PowerShell	PowerShell	PowerShell
Console de Gestion de IIS		Web-Metabase	Web-Metabase	Web-Metabase	Web-Metabase	Web-Metabase
		Web-Lgcy-Mgmt-Console	Web-Lgcy-Mgmt-Console	Web-Lgcy-Mgmt-Console	Web-Lgcy-Mgmt-Console	Web-Lgcy-Mgmt-Console
Composants spécifiques		ADLDS	Web-Server		Web-Server	Desktop-Experience
			Web-ISAPI-Ext		Web-ISAPI-Ext	
			Web-Basic-Auth		Web-Basic-Auth	
			Web-Digest-Auth			
			Web-Windows-Auth		Web-Windows-Auth	
			Web-Dyn-Compression			
Outlook Anywhere			RPC-over-HTTP- proxy			
Cluster					Failover-Clustering	

Dans ce tableau, les noms des composants Windows 2008 nécessaires sont indiqués avec le nom utilisable dans la commande `ServerManagercmd` dont voici la syntaxe :

```
servermanagercmd -i XXXX
```

Voici un exemple de script pour une installation classique d'un serveur de messagerie :

```
servermanagercmd -i Powershell
servermanagercmd -i web-metabase
servermanagercmd -i web-lgcy-mgmt-console
servermanagercmd -i web-server
servermanagercmd -i web-ISAPI-EXT
servermanagercmd -i web-basic-auth
servermanagercmd -i web-digest-auth
servermanagercmd -i web-windows-auth
servermanagercmd -i web-dyn-compression
```


© ENI Editions - All rigths reserved

```
servermanagercmd -i rpc-over-http-proxy
```

Aucune autre modification manuelle ne sera nécessaire sur Windows 2008 avant d'installer Exchange 2007.

Des informations complémentaires pourront être trouvées sur l'adresse http://technet.microsoft.com/en-us/library/bb691354.aspx

4. Les besoins propres à Exchange 2007

Voici les pré-requis à respecter afin de permettre l'installation d'Exchange 2007. Ces éléments seront vérifiés par le setup d'Exchange 2007 au moment de l'installation.

- Le maître de Schéma devra se trouver sur un serveur Windows 2003 SP1.
- Chaque site contenant au moins un serveur Exchange 2007 devra posséder un Catalogue Global hébergé par un serveur Windows 2003 SP1.
- Par ailleurs, au moins un contrôleur de domaine Windows 2003 (théoriquement en SP1) sera présent pour chaque domaine accueillant des utilisateurs associés à une boîte Exchange 2007. Cet aspect n'est pas très explicite dans la documentation Microsoft.
- La forêt et le domaine seront définis au minimum en mode Natif 2000.
- Les zones DNS utilisées par Active Directory seront configurées correctement. En particulier, les domaines sans extensions (**societe**. au lieu de **societe.local** par exemple) ne pourront pas être installés en Exchange 2007 SP1. L'installation d'Exchange 2007 sans SP1 sur Windows 2003 n'est pas une solution pérenne, puisque le passage du SP1 n'est pas possible non plus dans ces conditions.

À noter que le renommage de domaine Windows n'est pas supporté par Exchange 2007 (plus d'infos sur http://technet.microsoft.com/en-us/library/aa996719.aspx).

Bien entendu, un contrôleur de domaine Windows 2008 remplacera avantageusement un serveur Windows 2003 SP1.

Les combinaisons supportées :

	Système d'accueil	**Contrôleur sur les domaines**
Exchange Server 2007 SP1	Windows Server 2008	Windows Server 2008
Exchange Server 2007 SP1	Windows Server 2008	Windows Server 2003 SP1
Exchange Server 2007 SP1	Windows Server 2003 SP2	Windows Server 2008
Exchange Server 2007 SP1	Windows Server 2003 SP2	Windows Server 2003 SP1

Ceci n'empêche nullement d'avoir des serveurs Windows 2000 et Exchange 2000 dans la forêt. En revanche, Exchange 2000 devra être configuré (au niveau de l'onglet **Ds Access**) pour ne jamais utiliser de contrôleur de domaine 2008 !

À noter qu'il manque un patch pour installer Exchange 2007 sur Windows 2003 en français : **Update for Windows Server 2003 x64 Edition (KB918980)**. On conseillera donc toujours d'installer les versions anglaises (US) avec le kit de langue Française si cela s'avère nécessaire.

Exchange 2007, quelle que soit la langue installée, est multilingue, y compris dans son administration. Celle-ci s'adaptera automatiquement à la langue du système ou à la langue choisie par l'utilisateur sur les systèmes Windows multilangues.

5. Quelques recommandations sur l'architecture Active Directory

Pour les machines 32 bits, un ratio d'un contrôleur de domaine pour quatre serveurs Exchange possédant le rôle Mailbox est à préconiser. Attention, les machines Bi ou Quadri Pro comptent pour 2 et 4 dans ce ratio. Pour les machines 64 bits qui s'avèrent plus performantes, ce ratio est d'un contrôleur de domaine pour huit serveurs

© ENI Editions - All rigths reserved

Exchange.

Pour obtenir la meilleure optimisation possible, la mémoire des contrôleurs de domaine devrait permettre la mise en cache de la totalité de l'annuaire Active Directory. De manière approximative, on peut se baser sur la taille du fichier NTDS.DIT.

Il est préférable de limiter au maximum le nombre de sites contenant des serveurs Exchange 2007 ayant le rôle **Mailbox** puisque toutes les contraintes (Catalogue Global, rôle **Hub**) sont basées sur ce rôle. En effet, un serveur de catalogue global et un serveur possédant le rôle **Hub** sont nécessaires sur chaque site déclaré dans Active Directory possédant son serveur de boîtes aux lettres (Rôle Mailbox).

6. La procédure schématique d'installation

Il n'est pas possible de reprendre toutes les possibilités de combinaison d'installation. Chaque situation est bien particulière.

Chaque forêt et domaine qui accueilleront Exchange 2007 devront être préparés à partir d'un DVD Exchange 2007 sur un serveur Exchange 2007. Il est possible de préparer individuellement chaque domaine ou forêt ou de préparer l'intégralité. Le schéma devra être mis à jour en version Exchange 2007 :

```
SETUP /PREPARESCHEMA
```

Si tous les domaines suivent les recommandations, la commande suivante peut être utilisée :

```
SETUP /PREPAREALLDOMAINS
```

Sinon, chaque domaine peut être préparé séparément :

```
SETUP /PREPAREDOMAIN : Domaine.Extension
```

L'installation proprement dite des rôles Exchange peut aussi se réaliser facilement en ligne de commande !

```
SETUP /ROLES: MT, H, C, M
```

Cet exemple installe les outils d'administration Exchange et les rôles principaux d'accès, de transport et de banques d'information.

Voici les codes utilisables pour installer ou désinstaller chaque rôle :

- HubTransport, HT, H
- ClientAccess, CA, C
- Mailbox, MB, M
- UnifiedMessaging, UM, U
- EdgeTransport, ET, E
- ManagementTools, MT, T

Toute la configuration Exchange se fait à travers un contrôleur de domaine qu'il choisit en fonction de la configuration des sites et du réseau. Si le contrôleur choisi ne convient pas (s'il n'a pas le SP1, par exemple) , il faudra utiliser le paramètre `/DC:NomContrôleur.Domaine.Extension` pour utiliser un autre contrôleur de domaine.

7. Comment surveiller et optimiser Exchange ?

Le premier conseil est d'utiliser l'outil **EXBPA** (*Exchange Best Practices Analyzer*) qui est intégré à Exchange 2007, et qui permet de corriger un certain nombre d'erreurs classiques de configuration aussi bien dans Windows et Active Directory que dans Exchange ! Même si son usage devient de plus en plus rare, ESEUTIL est utilisé ponctuellement pour vérifier l'état des bases. Les erreurs corrigées sont aussi moins nombreuses que dans les anciennes versions.

Les outils de surveillance classique :

© ENI Editions - All rigths reserved

- l'analyseur de Performances de Windows,
- l'outil d'analyse du réseau **Network Monitor**.

On peut aussi installer et configurer le composant **Windows System Resources Manager** de Windows 2008. Celui-ci doit se trouver sur le serveur Exchange lui-même.

L'outil Microsoft SCOM 2007 (ou MOM 2005) est évidemment très couramment utilisé dans ce type de configuration. Attention, le choix de la langue et des paramètres régionaux (point et virgule) peuvent avoir un impact **négatif** sur l'évaluation de certains compteurs de performances. Des adaptations sont à prévoir de ce côté pour éviter des alertes intempestives.

8. Quelques points particuliers à prendre en compte

Attention si les contrôleurs de domaines ne sont pas en langue anglaise ! Si vous prévoyez d'utiliser **Outlook Web Access** dans votre organisation, vous devrez installer le patch décrit dans l'article 919166. La fonctionnalité **Carnet d'adresse** de Exchange 2007 est inopérante quand le client Exchange **OWA** et le contrôleur de domaine Windows 2003 (ou Windows 2008) n'ont pas été configurés avec les mêmes paramètres régionaux.

La migration d'un cluster 2003, même déjà en Exchange 2007, ne peut se faire que vers un nouveau cluster 2008. La classique mise à jour **in place**, nœud par nœud, ne sera pas possible.

Les serveurs **RODC** (contrôleur de domaine en lecture uniquement) ne sont pas utilisables par Exchange 2007. Il ne serait pas logique (mais pas impossible) d'installer un serveur Exchange 2007 sur un site ne possédant qu'un RODC, puisque cela revient à faciliter la capture de nombreuses données.

La sauvegarde !!! On ne peut plus compter sur Ntbackup (ni sur Windows Backup)! En effet, les périphériques de type **streamer** ne sont plus gérés, et Exchange n'est tout simplement pas vu, ni géré de manière adéquate. La solution préconisée serait donc soit d'utiliser Data Protection Manager (de Microsoft) ou d'acheter un logiciel de sauvegarde chez un des nombreux fournisseurs qui se sont penchés sur cette question. La question est en cours chez Microsoft.

Après ces petits inconvénients à prendre en compte, il est important d'indiquer tous les apports de Windows 2008.

9. Les avantages à utiliser Exchange Server 2007

Exchange 2007 SP1 est pour le moment la seule messagerie à fonctionner sur Windows 2008 !

a. Les avantages spécifiques de Windows 2008 pour Exchange 2007

Les améliorations d'Active Directory (surtout en 64 bits) permettent très souvent de conserver en mémoire la totalité de l'annuaire. L'accès **natif** aux SAN/Storages (iScsi,…) est un plus important, ce qui facilite l'installation initiale et l'ajout d'espaces disques au fur et à mesure que les besoins évoluent.

La virtualisation sur **HyperV** qui est maintenant supportée (http://technet.microsoft.com/en-us/library/cc794548.aspx) autorise de nouvelles topologies de configuration pour un support et des reprises d'activités plus rapides.

Le cluster de type **Failover** pourra être réparti géographiquement, sans être obligé de créer et gérer des VLANs. Ceci est maintenant possible, par l'ajout de plusieurs adresses IP (une par réseau) sur les ressources partagées.

Un meilleur support de IPv6 pour l'accès depuis le réseau local, même si IPv4 reste pour le moment indispensable au bon fonctionnement (http://technet.microsoft.com/en-us/library/bb629624.aspx).

Windows 2008 permet plus facilement de n'installer que les composants systèmes nécessaires.

b. D'autres exemples d'améliorations

Exchange 2007 sur Windows 2003 est limité par le nombre de ports TCP utilisables entre les serveurs CAS et les serveurs Mailbox. Windows 2008 permet de contourner le problème en utilisant un pool de connexions RPC. Ceci pouvait limiter à 6000 clients OWA utilisant chacun 6 à 10 connexions TCPs.

Windows 2008 possède aussi des compteurs supplémentaires intéressants dont voici quelques exemples significatifs :

© ENI Editions - All rigths reserved

- Current Number of Incoming RPC over HTTP Connections
- Current Number of unique users
- RPC/HTTP requests per second
- Number of Failed Back-End Connection attempts per Second

Ces paramètres de performances apparaîtront en anglais si vous installez vos systèmes en versions multilingues basées sur l'anglais tel que cela est fortement conseillé. L'installation de version purement française est actuellement complexe mais possible en téléchargeant un patch spécifique sur le site MSDN des développeurs.

La liste complète des compteurs pourra être trouvée à l'adresse suivante : http://technet.microsoft.com/en-us/library/cc540453.aspx

Exchange 2007 est donc la messagerie privilégiée sur Windows 2008. En revanche, il faut voir la messagerie SMTP comme complémentaire pour l'optimisation, le filtrage et la sauvegarde de toute messagerie.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre est consacré à la définition et la configuration des composants nécessaires au bon fonctionnement d'un réseau d'entreprise basé sur Windows 2008.

Les composants IP, DNS, DHCP, WINS, ainsi que la mise en place de la quarantaine réseau sur DHCP, IPSEC et 802.1x seront abordés.

© ENI Editions - All rigths reserved

L'implémentation d'un système d'adressage IP

La mise en place de toute architecture réseau passe par l'analyse des réseaux existants. Il est souvent difficile de modifier l'ensemble en une seule fois. La migration se fait donc souvent en implémentant un nouvel adressage réseau et une cohabitation avec les réseaux existants. La modification de l'adressage IP est souvent vue comme une modification coûteuse, n'apportant que peu d'avantages supplémentaires.

Le changement d'un domaine DNS est encore plus compliqué, surtout lorsque ce domaine DNS sert de support à un domaine Active Directory. Dans ce cas, une migration représente une étude particulière qui sort du cadre de cette présentation.

1. Le choix de l'architecture réseaux

Deux point précis sont à étudier à ce niveau :

- le choix de la zone DNS ;
- le choix de la classe réseau.

a. La zone DNS

Deux aspects sont importants lors du choix de la zone DNS.

Le nom de la zone DNS choisi doit correspondre à l'intégralité de l'entité (Entreprise, Groupe, etc.) que l'on souhaite gérer. Ce nom doit pourvoir être accepté par toutes les entités dépendantes qui vont se retrouver dans cette zone. Le problème est beaucoup plus politique que technique !

Si une entité n'entre pas dans ce cadre, cela veut dire qu'une zone DNS spécifique devra lui être affectée.

Si la zone DNS doit être utilisée sur Internet, le domaine DNS sera forcément public et enregistré, c'est-à-dire utilisant une extension reconnue de type " .FR, .COM .INFO… " !

En revanche, pour un réseau interne, le domaine peut être public ou privé. Le choix le plus courant est alors d'utiliser un domaine DNS local avec une extension inconnue sur Internet. L'extension **.local** est très souvent utilisée sous la forme **MaSociete.local**. Le découpage entre ce qui est interne ou externe est plus facile à sécuriser. En revanche, l'utilisation d'un même nom suppose une double administration, donc plus complexe, de serveurs DNS différents pour ne rendre visible sur Internet que ce qu'il est souhaitable de montrer.

b. La classe réseau

Pour tous les réseaux internes, le choix se portera évidemment toujours sur les classes réseaux privées. Si l'on ne peut pas toujours modifier l'intégralité des réseaux existants pour des raisons souvent historiques, on peut au moins créer tous les nouveaux réseaux en suivant cette règle.

La classe du réseau se choisit en fonction du nombre de machines présentes sur le réseau, du nombre de sites, etc. Un réseau de classe C (192.168.0.X) représente souvent le bon choix initial. Il est toujours possible de changer de classe, de réseau ou même surtout d'utiliser plusieurs réseaux en fonction des besoins.

L'usage de TCPIPv6 n'est pas encore bien développé mais deviendra nécessaire dans les 2 ou 3 années qui suivent, principalement sur Internet. Sur le réseau local, il reste encore de nombreux logiciels qui ne sont pas compatibles, mais ceci devrait évoluer très rapidement !

2. L'installation d'un serveur DHCP

Si le service DHCP permet de mettre en place rapidement le réseau choisi, il permet aussi de modifier rapidement et globalement une série de paramètres. Il reste encore quelques irréductibles qui n'utilisent pas ce service, c'est maintenant rarissime.

Parmi les nombreux composants de Windows 2008, le service DHCP est un rôle.

a. Définition

Le protocole DHCP (*Dynamic Host Configuration Protocol*) a pour but de fournir une adresse IP et un masque à tout

© ENI Editions - All rigths reserved

périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la configuration, d'autres paramètres tous aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser, des serveurs WINS et le suffixe de domaine, pour ne citer que les principaux.

DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs.

b. L'installation

Comme pour tous les composants Windows, l'installation peut se faire graphiquement ou en mode commande sans avoir besoin d'insérer le moindre média.

```
servermanagercmd -install DHCP
```

Attention, le service devra être mis en démarrage automatique !

```
sc \\%COMPUTERNAME% config DHCPServer start= auto
```

Le service peut ensuite être démarré de manière classique :

```
NET START DHCPSERVER
```

Le démarrage du service permet de le rendre accessible et configurable.

Pour que le service DHCP commence à distribuer des adresses, il est indispensable de configurer et d'activer une étendue.

Attention, si le serveur qui héberge DHCP fait partie d'une forêt Active Directory, il doit en plus avoir été autorisé par des administrateurs membres du groupe « Administrateurs de l'entreprise » ou ayant reçu les droits d'administration DHCP.

Le service DHCP comme les autres services réseaux de références (DNS, WINS) devraient toujours être installés sur des serveurs disposant d'adresses IP fixes.

c. La configuration

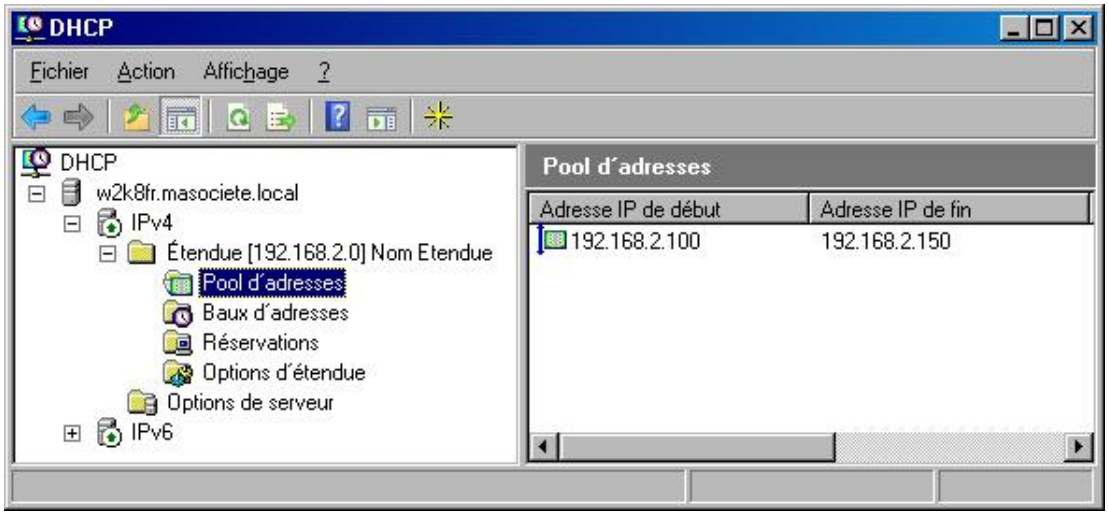
La console d'administration DHCP est automatiquement installée en même temps que le service, mais peut aussi être lancée à partir de toute autre machine possédant cette console.

Même sur le serveur lui-même, sélectionnez le serveur DHCP (ou les serveurs) que vous souhaitez gérer. La liste des serveurs déjà autorisés s'affiche automatiquement.

- Pour autoriser un serveur DHCP, utilisez l'option **Gérer les serveurs autorisés**, puis cliquez sur le bouton **Autoriser**, et saisissez le nom ou l'adresse IP.

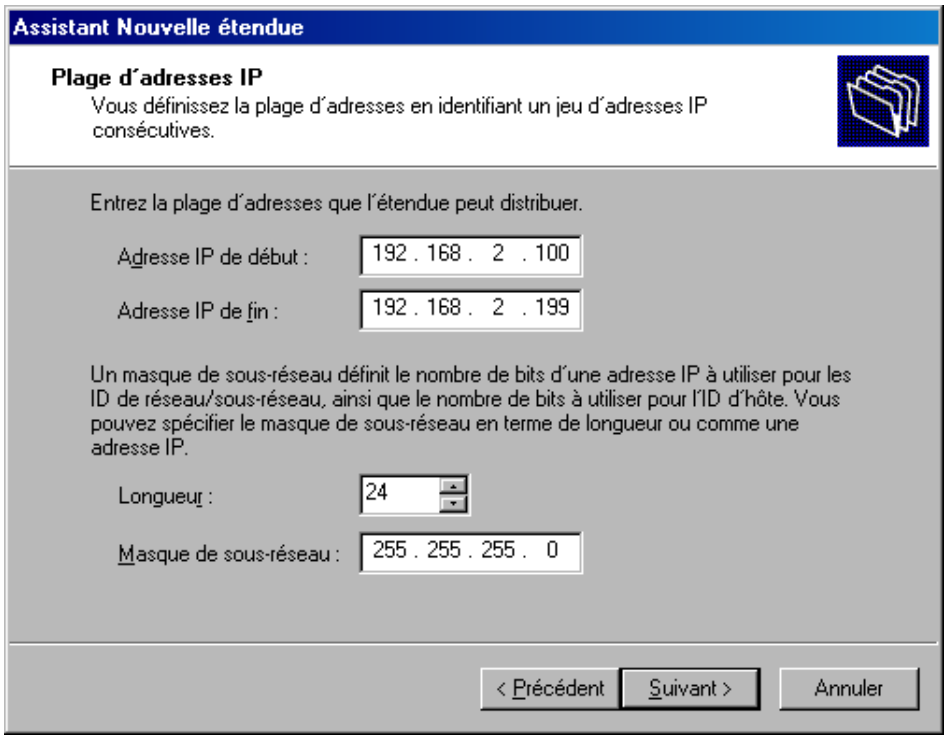
  Les serveurs autorisés apparaissent avec une flèche verte.

© ENI Editions - All rigths reserved



Chaque serveur DHCP peut servir de nombreuses étendues, mais une seule pour chaque réseau IP.

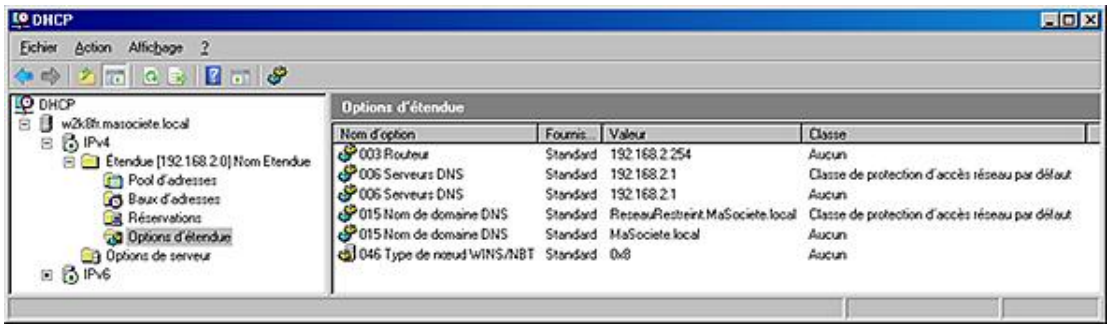
Voici une étendue classique pour un réseau 192.168.2.X de classe C utilisant le masque standard 255.255.255.0 !


Assistant Nouvelle étendue
Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.
Entrez la plage d'adresses que l'étendue peut distribuer.
Adresse IP de début : 192 . 168 . 2 . 100
Adresse IP de fin : 192 . 168 . 2 . 199
Un masque de sous-réseau définit le nombre de bits d'une adresse IP à utiliser pour les ID de réseau/sous-réseau, ainsi que le nombre de bits à utiliser pour l'ID d'hôte. Vous pouvez spécifier le masque de sous-réseau en terme de longueur ou comme une adresse IP.
Longueur : 24
Masque de sous-réseau : 255 . 255 . 255 . 0
< Précédent
Suivant >
Annuler

La plage utilisée ne doit pas forcément utiliser la totalité de la classe réseau afin de laisser de la place pour les serveurs, les adresses IP réservées pour les imprimantes.

La route par défaut fait partie des paramètres habituels liés à l'étendue.

Les options au niveau du serveur contiennent les paramètres qui sont valables globalement sur toutes les étendues.



© ENI Editions - All rigths reserved

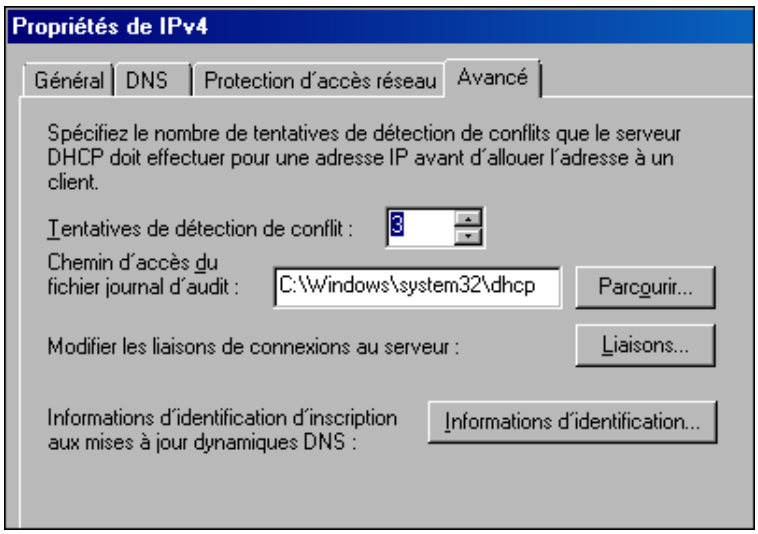
Les options Serveurs (005,006,015,046) servent de valeur par défaut, mais sont remplacées par les options de l'étendue qui ont priorité.

- La zone **Nom de domaine DNS** ne permet pas de spécifier plusieurs suffixes de recherche DNS. Si nécessaire, les stratégies proposent d'ajouter des suffixes de recherche.

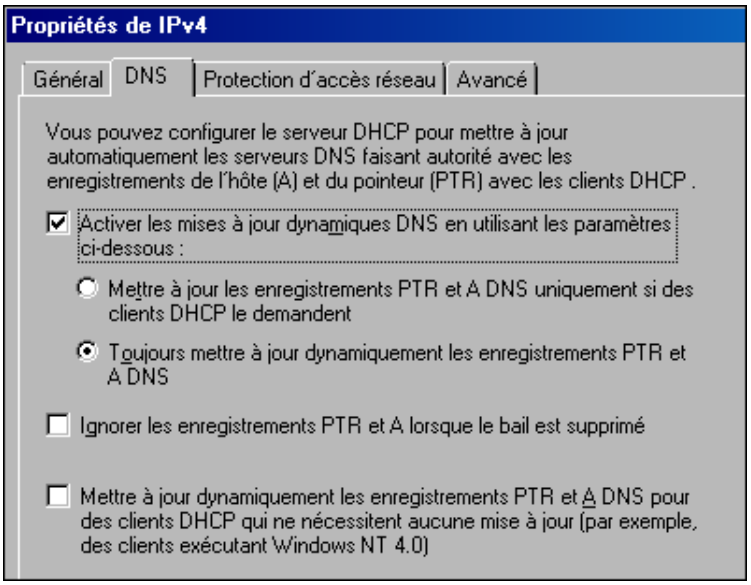
- Le **Type de Nœud** avec la valeur 0x8 configure le mode de résolution hybride. C'est-à-dire qu'une interrogation des serveurs DNS/WINS sera faite en premier, avec bascule en mode Broadcast en cas d'échec.

Certaines propriétés avancées du serveur DHCP peuvent être très intéressantes à configurer.

Par exemple, lorsque la zone **Tentatives de détection de conflit** est configurée avec une valeur supérieure à zéro, DHCP utilisera l'instruction **ping** pour déterminer l'existence éventuelle d'une machine sur cette adresse.


Propriétés de IPv4
Général
DNS
Protection d'accès réseau
Avancé
Spécifiez le nombre de tentatives de détection de conflits que le serveur DHCP doit effectuer pour une adresse IP avant d'allouer l'adresse à un client.
Tentatives de détection de conflit :
3
Chemin d'accès du fichier journal d'audit :
C:\Windows\system32\dhcp
Parcourir...
Modifier les liaisons de connexions au serveur :
Liaisons...
Informations d'identification d'inscription aux mises à jour dynamiques DNS :
Informations d'identification...

La mise à jour dynamique des DNS est un élément particulièrement important à gérer.


Propriétés de IPv4
Général
DNS
Protection d'accès réseau
Avancé
Vous pouvez configurer le serveur DHCP pour mettre à jour automatiquement les serveurs DNS faisant autorité avec les enregistrements de l'hôte (A) et du pointeur (PTR) avec les clients DHCP.
Activer les mises à jour dynamiques DNS en utilisant les paramètres ci-dessous :
Mettre à jour les enregistrements PTR et A DNS uniquement si des clients DHCP le demandent
Toujours mettre à jour dynamiquement les enregistrements PTR et A DNS
Ignorer les enregistrements PTR et A lorsque le bail est supprimé
Mettre à jour dynamiquement les enregistrements PTR et A DNS pour des clients DHCP qui ne nécessitent aucune mise à jour (par exemple, des clients exécutant Windows NT 4.0)

Lorsque les zones de recherche inverses (Reverse ARP) sont créées et utilisées, il est important de mettre à jour les enregistrements PTR et de ne pas les ignorer lorsque le bail est supprimé.

La durée du bail sera d'autant plus longue que le nombre d'adresses IP disponibles est important et que le risque de conflit est limité.

d. Les réservations

Même chez les administrateurs qui voudraient gérer toutes les machines en adressage IP fixe, DHCP peut être très utile. En effet, certains gèrent ainsi la totalité du parc avec une réservation pour chaque adresse IP, même si ceci

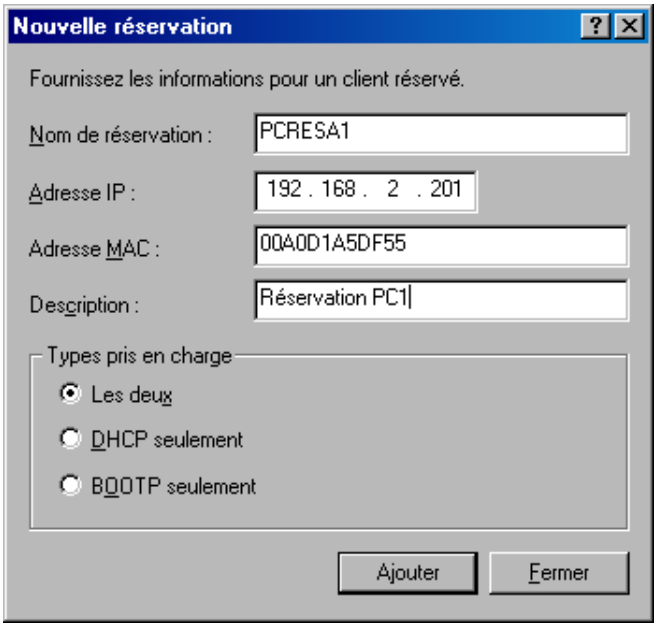
© ENI Editions - All rigths reserved

représente une sécurité plus que fictive.

Sans aller jusqu'à gérer tout le réseau, les réservations sont très utiles pour les imprimantes réseau, les périphériques particuliers administrables (switch…) et parfois pour certaines machines dont l'adresse IP a été autorisée et utilisée dans la configuration d'un logiciel.

Chaque carte réseau disposant d'une adresse physique unique appelée **Mac Address**, il est possible d'identifier la demande provenant de cette adresse, et de lui fournir toujours la même adresse IP et la même configuration.

Voici un exemple de définition de réservation :



À noter que les réservations doivent faire partie du réseau, mais pas de l'étendue DHCP, ce qui peut parfois être très pratique. Si plusieurs DHCP sont utilisés pour un même réseau (avec les restrictions d'usages), les réservations doivent être configurées sur tous ces serveurs.

Certains outils provenant des kits de ressources comme DHCPCMD.EXE, ou la librairie DHCPOBJS.DLL permettent de développer des scripts pour automatiser la création et la configuration des étendues. La commande `NETSH` permet aussi de réaliser certaines opérations de configuration, d'import et d'export.

Après avoir enregistré la dll DHCPOBJS.DLL par la commande `Regsvr32 DHCPOBJS.DLL`, voici un exemple de script que l'on peut utiliser pour créer une étendue :

```
On Error resume next

Set dhcpmgr= createObject("Dhcp.Manager")
IPNET="192.168.2"

Set dhcpsrvr = dhcpmgr.Servers.Connect(IPNET&".1")
dhcpsrvr.Scopes.Add IPNET&".100", IPNET&".150", _
"255.255.255.0", "Nom Etendue", "Description Etendue", True

dhcpsrvr.Scopes(1).Options.Add 3, Array(IPNET&".254")
dhcpsrvr.Scopes(1).Options.Add 6, Array(IPNET&".1")
dhcpsrvr.Scopes(1).Options.Add 15, "MaSociete.Local"
dhcpsrvr.Options.Add 46, cbyte(8)
dhcpsrvr.Disconnect
```

© ENI Editions - All rigths reserved

La mise en place des systèmes de résolutions de nom

1. La résolution DNS

DNS est devenu la pierre de base du fonctionnement d'un réseau Windows basé sur Active Directory, mais pas seulement.

La plupart des activités actuelles (Messagerie, Internet) sont basées sur le bon fonctionnement du réseau et en particulier du module DNS.

Il n'est donc maintenant plus possible de se passer de ce système qui héberge de plus en plus d'informations vitales au bon fonctionnement de l'ensemble du réseau.

a. Définition

DNS (*Domain Name Server*) correspond tout d'abord à un protocole permettant à des clients (du réseau) d'interroger une base de données contenant des informations sur les machines et les services hébergés par ces machines.

DNS est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine

b. L'installation

L'installation du service DNS sur un réseau Windows se fait souvent dans le cadre de l'installation du premier contrôleur de domaine Active Directory. Sa configuration initiale est alors automatiquement prise en charge par l'assistant DCPROMO. Par défaut, la zone DNS utilisée par Active Directory est alors intégrée et gérée par Active Directory.

Si l'on doit automatiser ou ajouter un service DNS, voici l'instruction à utiliser :

```
servermanagercmd -install DNS
```

Si le service DNS est ajouté sur un contrôleur de domaine, alors toutes les zones intégrées à Active Directory sont connues et utilisées par le service DNS pour sa résolution.

Dans tous les autres cas, le service DNS devra être géré comme un serveur DNS classique. Il pourra alors héberger des zones et servir de cache ou de renvoi vers d'autres systèmes DNS.

c. Les différents types de zones

La zone de type Principale

Bien entendu, ce type de zone sera surtout utilisé pour gérer des zones non liées à AD. Les zones DNS publiques, contenant les serveurs Web de l'entreprise et les serveurs de messagerie, sont les exemples les plus courants d'utilisation.

Chaque zone est sauvegardée dans un fichier texte spécifique au format tout à fait standard avec l'extension .DNS. Ce type de fichier est compatible avec les autres systèmes DNS très connus comme BIND. Ceci autorise l'importation ou l'exportation de zones DNS entre différents serveurs.

Le serveur qui héberge la zone principale est le seul à autoriser et valider les mises à jour de sa zone. C'est la principale différence avec les zones intégrées à AD qui elles autorisent les modifications sur chaque contrôleur.

La zone de type Secondaire

Une zone secondaire peut être établie à partir d'un serveur de zone principale, d'une zone intégrée à Active Directory ou même d'un autre serveur de zone secondaire. La zone secondaire n'est qu'une réplique exacte de la zone dont elle dépend. En revanche, la réplication doit avoir été autorisée sur le serveur servant de référence.

Dans le monde Windows, la zone de type secondaire sert très souvent à répliquer les informations d'un autre domaine AD afin de réaliser une approbation entre deux domaines. Les zones secondaires sont souvent configurées sur des serveurs BIND (Unix ou Linux) pour obtenir une résolution indirecte des domaines DNS gérés par AD.

Comme la zone principale, les informations sont sauvegardées dans un fichier texte utilisant l'extension .DNS

© ENI Editions - All rigths reserved

En cas de perte du serveur principal, un serveur de zone secondaire peut devenir un nouveau serveur principal.

Les zones secondaires présentent souvent des problèmes de réplication, de délais de mise à jour, de notification et de sécurité à configurer, qu'il vaut mieux éviter.

La zone intégrée à Active Directory

La zone intégrée à Active Directory consiste, comme le nom l'indique, à utiliser la base de données Active Directory comme réceptacle de l'information. Du coup, celle-ci bénéficie de toutes les options de sécurité de AD, ainsi que de la réplication incrémentale entre tous les contrôleurs de domaine.

Tous les domaines DNS peuvent être intégrés à AD, et pas seulement ceux utilisés par AD.

Sauf cas particuliers, toutes les zones DNS ont intérêt à être intégrées à AD.

d. Les différents types de réplications

Ceux-ci ne s'appliquent qu'aux zones intégrées à AD en accédant aux propriétés du domaine choisi.

La réplication sur tous les serveurs DNS de la forêt

Cette réplication est à préconiser pour les domaines qui ont intérêt à être connu (et résolu) rapidement sur tous les domaines de la forêt sans avoir à transférer les requêtes vers ce que l'on appelle les **redirecteurs** (Forwarders). Ce choix s'applique particulièrement au domaine racine de la forêt.

La réplication sur tous les contrôleurs du domaine

La réplication sur tous les contrôleurs du domaine est le mode compatible avec ce qui se faisait sur Windows 2000. C'est le choix logique lorsque seuls les contrôleurs de domaine sont utilisés comme serveurs DNS de référence. En effet, comme les contrôleurs de domaine répliquent déjà les données DNS au même titre que les autres données de l'annuaire, il suffit d'installer le service DNS pour qu'ils assurent cette fonction.

La réplication sur tous les serveurs DNS du domaine

Ce choix est rarement utilisé, et permet à des serveurs DNS qui ne sont pas contrôleurs de domaine de recevoir aussi la réplication d'une zone précise.

- Sélectionnez la zone DNS, puis cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** dans le menu.

- Cliquez sur le bouton **Modifier** en face de **Réplication**.

Les différents types de réplications apparaissent.

La réplication liée à une partition souvent dite applicative

Par défaut, dans une forêt AD, il existe déjà deux partitions applicatives particulières de ce type et qui sont déjà proposées pour la réplication :

- la ForestDnsZones ;

- la DomainDnsZones.

Si une autre partition applicative a été créée, celle-ci peut être utilisée pour répliquer des informations DNS (ou autres) sur des groupes de machines personnalisés.

À noter qu'en cliquant droit sur le serveur DNS, l'option **Créer des partitions de l'annuaire d'applications par défaut** peut s'avérer utile pour recréer l'une ou l'autre des partitions.

e. Les zones reverses (dites de recherches inversées)

Les zones reverses ARP recherchent le nom d'une machine à partir de l'adresse IP. Le classement est donc fait en fonction de l'adressage réseau IP.

Ce mode de recherche n'est pas nécessaire et n'est pas utilisé pour le fonctionnement normal d'une forêt Active Directory. C'est pour cette raison que Microsoft ne crée pas automatiquement de zones reverses

En revanche, le client DNS Microsoft sait bien entendu l'utiliser si elle est définie. Certains logiciels comme la sauvegarde **TINA** (*Time Navigator de ATEMPO*) ont un besoin impératif de ce type de zone pour fonctionner

© ENI Editions - All rigths reserved

correctement.

Lors de la résolution de problème réseau et de l'utilisation de l'outil NsLookup, il est indispensable d'avoir créé les zones reverses pour le bon fonctionnement de cet outil et la bonne interprétation des résultats.

Comme les zones classiques dites de **recherches directes**, il est possible de créer des zones principales (intégrées ou non à AD) ou des secondaires.

Dès que ces zones sont créées, il est important de configurer DHCP pour gérer les mises à jour des enregistrements **PTR**, c'est-à-dire nom d'hôte associé à chaque adresse IP. L'intégration de ces zones à AD se fera surtout pour les réseaux IP qui contiennent majoritairement des machines Windows.

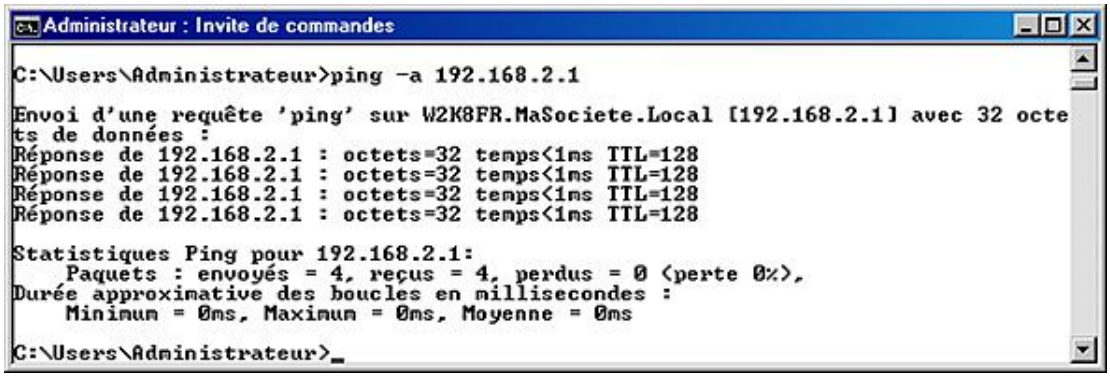
Lors de la création d'une zone de recherche inverse, le nom de la zone est basé sur l'adressage IP donc chaque valeur est prise à l'envers. À noter qu'une zone inverse peut aussi être intégrée ou non, principale ou secondaire…

f. Les tests et vérifications

Différents outils sont utilisables pour vérifier le bon fonctionnement de la résolution sur les différents domaines :

L'outil **ping** est la première étape à réaliser pour les tests de résolution. Attention, le résultat des tests peut être perturbé par le filtrage existant sur les pare-feu intermédiaires ou sur les systèmes eux-mêmes. Utilisez **ping** avec le nom court, le nom complet (nom suivi du domaine DNS complet) et l'adresse IP. Si une réponse est obtenue sur chacun de ces tests, tout est pour le mieux. Dans le cas de l'adresse IP, l'argument `-a` permet aussi de vérifier la résolution inverse.

Si le nom complet **W2K8FR.MaSociete.Local** apparaît, c'est que la résolution inverse fonctionne bien, même dans le cas où il n'y a pas de réponse au ping.


Administrateur : Invite de commandes
C:\Users\Administrateur>ping -a 192.168.2.1
Envoi d'une requête 'ping' sur W2K8FR.MaSociete.Local [192.168.2.1] avec 32 octets de données :
Réponse de 192.168.2.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.1 : octets=32 temps<1ms TTL=128
Statistiques Ping pour 192.168.2.1:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\Administrateur>_

L'outil **NsLookup** permet d'interroger les serveurs DNS sur tous les différents champs et enregistrements des zones DNS accessibles.

Les deux commandes `Tracert` et `PathPing` sont un équivalent du ping, mais qui indique toutes les étapes, les adresses traversées et les durées de chaque étape.

Bien entendu, d'autres outils comme **netsh**, **dnscmd**, et **dcdiag** complètent énormément les possibilités.

Vous trouverez également des informations complémentaires sur l'implémentation de l'Active Directory dans le chapitre Domaine Active Directory.

g. Les différents types d'enregistrements

SOA : l'enregistrement de type SOA correspond à la source de l'autorité de la zone concernée. Toutes les modifications dans la zone incrémente un numéro de version associé à cette zone.

NS : l'enregistrement NS contient tous les serveurs de noms de serveurs autorisés à répondre pour ce domaine.

Contrairement aux autres enregistrements, les enregistrements SOA et NS sont uniques dans chaque zone.

A : l'enregistrement A définit l'adresse IP associée à un nom de machine (appelée hôte ou Host en anglais) bien précis.

CNAME : l'enregistrement CNAME crée un nom (appelé Alias) dans une zone, qui pourra être associé à un enregistrement de type A dans la même zone ou même dans une autre zone DNS.

MX : chaque enregistrement MX doit pointer sur un enregistrement de type A donc une machine possédant un service SMTP actif. Cet enregistrement est totalement inutile pour la messagerie interne basée sur Exchange. Lorsque plusieurs enregistrements de type MX existent, le poids (ou priorité) le plus faible affecté à chacun d'eux indique le serveur de messagerie à utiliser en priorité.

SRV : l'enregistrement SRV a pour fonction d'indiquer un service particulier qui sera rendu sur le port spécifié. Les

© ENI Editions - All rigths reserved

services LDAP, Catalogue Global, Kerberos, SIP et bien d'autres sont basés sur ce type d'enregistrement.

PTR : ce type d'enregistrement est le pendant du type A. Il n'existe que dans les zones de recherches inversées.

D'autres types existent comme le champ TXT qui sont plus rarement utilisés et peu utiles dans le fonctionnement de Windows.

h. Les bons usages

Dans le cadre de forêts Active Directory, les bonnes pratiques sont d'éviter les réplications inutiles d'informations, et donc d'éviter l'usage de zones secondaires à l'origine de nombreux problèmes.

Les deux solutions à utiliser sont les stubs zones ou les redirections conditionnelles.

Pour les forêts et réseaux complexes, la simplification passe par l'utilisation de redirecteurs au niveau de chaque sous-domaine vers le domaine racine de chaque forêt.

Au niveau de chaque domaine racine de chaque forêt, l'utilisation d'une redirection conditionnelle vers chaque forêt suffira pour résoudre toute la forêt correspondante.

2. La résolution WINS

En théorie, cette résolution ne devrait plus être utilisée sauf pour intégrer d'anciens domaines NT4. En pratique, il arrive que celle-ci soit nécessaire (voire très pratique) pour certaines vieilles applications Microsoft ou non, mais aussi pour des applications très récentes comme Exchange 2007 (dans des cas très particuliers).

Lors de migration ou lorsqu'il y a un doute pour le fonctionnement de certaines applications, il est courant de garder un ou deux serveurs WINS sur le site central. Les stations et serveurs utilisant ce type d'application pointeront directement sur ce serveur WINS. Il est ainsi inutile de maintenir et de répliquer les serveurs WINS à travers tout le réseau.

a. Définition

WINS (*Windows Internet Naming Service*) est un service basé sur une base de données Jet permettant de retrouver l'adresse IP d'un nom Netbios, et réciproquement.

Contrairement à DNS, WINS maintient des informations sur les groupes de machines, mais aussi sur les utilisateurs connectés aux machines.

b. L'installation

L'installation de WINS se fait par l'ajout de la fonctionnalité correspondante :

```
servermanagercmd -install WINS-Server
```

c. La configuration

Sauf cas rare où il faut entrer manuellement un nom (dit statique) et une adresse IP, il n'est pas nécessaire de configurer un serveur WINS qui reçoit dynamiquement toute l'information nécessaire par le serveur et les clients qui s'inscrivent automatiquement dans la base.

Le seul élément particulier de la réplication consiste à répliquer la base entre deux serveurs WINS, voire plus dans certains cas.

d. La réplication entre WINS

La réplication WINS est basée sur deux opérations : l'émission et la collecte.

Pour qu'une réplication WINS fonctionne dans un sens, un serveur WINS doit être configuré pour émettre les modifications qu'il reçoit vers un autre serveur WINS, mais il faut aussi que l'autre serveur WINS soit configuré pour collecter les informations en provenance du serveur émetteur précis.

Pour une réplication fonctionnant dans les deux sens entre deux serveurs WINS, il faut et il suffit que chaque serveur soit configuré en mode **Emission/Collecte** pour le serveur distant.

© ENI Editions - All rigths reserved

e. Quand et pourquoi utiliser WINS ?

Attention, il ne faut plus voir WINS comme une solution à part entière. Car DNS est maintenant indispensable.

WINS est simplement une solution pour résoudre des problèmes marginaux de fonctionnement d'applicatifs ou d'accès qu'il serait trop complexe de résoudre autrement.

Le cas le plus concret, comme pour Exchange dans certaines parties, est le logiciel qui n'a prévu que des noms de serveurs **simples** et relativement **courts**.

L'installation d'un service WINS unique, centralisé qui ne serait utilisé que par les quelques stations ou serveurs qui en ont vraiment besoin répond très bien à ce type de problème.

© ENI Editions - All rigths reserved

La mise en place de la quarantaine réseau

La quarantaine réseau n'est pas une véritable solution de sécurité, mais c'est un élément dont l'objectif est de maintenir en bonne santé les éléments présents sur le réseau.

1. La préparation de l'environnement commun aux différents types de quarantaine

L'utilisation du client NAP (*Network Access Protection*) est basée sur l'utilisation d'un NPS (*Network Policy Server*), c'est-à-dire un serveur de stratégies réseau, qui permet de définir des restrictions souhaitées.

Il est donc nécessaire d'installer et de configurer ce rôle :

```
servermanagercmd -install NPAS-Policy-Server
```

Après installation, différents points sont à définir pour des stratégies fonctionnelles :

- un système de validation (SHV), c'est-à-dire de tests à réaliser pour vérifier un système ;
- un groupe de serveurs de **remediation** : ce sont les serveurs vus et autorisés par les stations non conformes afin de se mettre à jour ;
- des stratégies de **santé**, qui définissent comment les SHVs sont interprétés ;
- des stratégies de réseau.

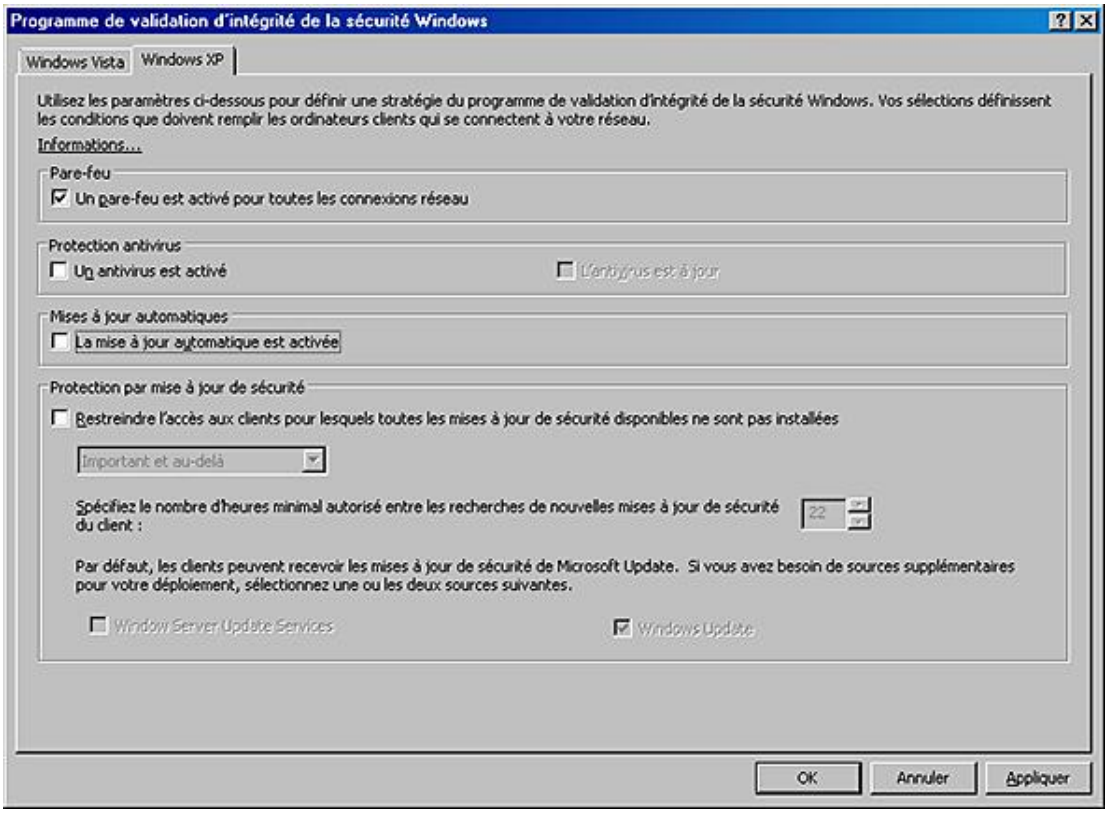
Le kit d'intégration **ForeFront for NAP** (gratuit) sera téléchargé afin de disposer d'un système de validation complémentaire. Différents modules seront chargés sur les machines en fonction du type de processeurs (32 ou 64 bits), le module SHV sur les serveurs NPS, le module SHA sur les clients à valider.

La première étape consiste à définir les tests que l'on souhaite réaliser sur les machines disposant du client NAP, c'est-à-dire Windows XP SP3 ou Windows Vista.

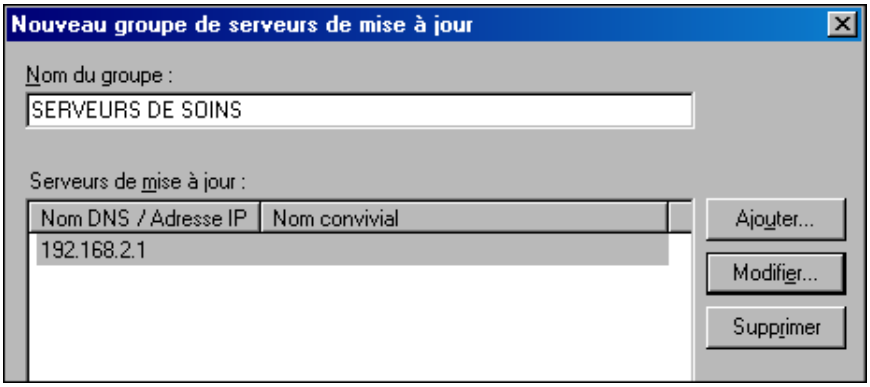
- Dans l'administration du serveur NPS, **Protection d'accès réseau**, sélectionnez le conteneur **Programmes de validation d'intégrité système**.
- Configurez ensuite le système de validation fourni par défaut appelé **Validateur d'intégrité de la sécurité Windows**.
- Dans les paramètres principaux, on considère que si les programmes de validation d'intégrité ne répondent pas ou ne peuvent pas répondre, le client sera réputé **Non Conforme**. Mais pour chaque situation, l'adaptation du statut est modifiable.
- Cliquez sur le bouton **Configurer** pour accéder aux propriétés à tester. À noter qu'il y a un onglet différent pour XP et pour Vista.

Dans le cadre de cette mise en place de tests, une configuration simplifiée basée sur la présence du pare-feu sera utilisée !

© ENI Editions - All rigths reserved


Programme de validation d'intégrité de la sécurité Windows
Windows Vista
Windows XP
Utilisez les paramètres ci-dessous pour définir une stratégie du programme de validation d'intégrité de la sécurité Windows. Vos sélections définissent les conditions que doivent remplir les ordinateurs clients qui se connectent à votre réseau.
Informations...
Pare-feu
Un pare-feu est activé pour toutes les connexions réseau
Protection antivirus
Un antivirus est activé
L'antivirus est à jour
Mises à jour automatiques
La mise à jour automatique est activée
Protection par mise à jour de sécurité
Restreindre l'accès aux clients pour lesquels toutes les mises à jour de sécurité disponibles ne sont pas installées
Important et au-delà
Spécifiez le nombre d'heures minimal autorisé entre les recherches de nouvelles mises à jour de sécurité du client :
22
Par défaut, les clients peuvent recevoir les mises à jour de sécurité de Microsoft Update. Si vous avez besoin de sources supplémentaires pour votre déploiement, sélectionnez une ou les deux sources suivantes.
Window Server Update Services
Windows Update
OK
Annuler
Appliquer

La deuxième étape consiste à définir un groupe contenant les serveurs autorisés pour réaliser sa remise aux normes demandées.

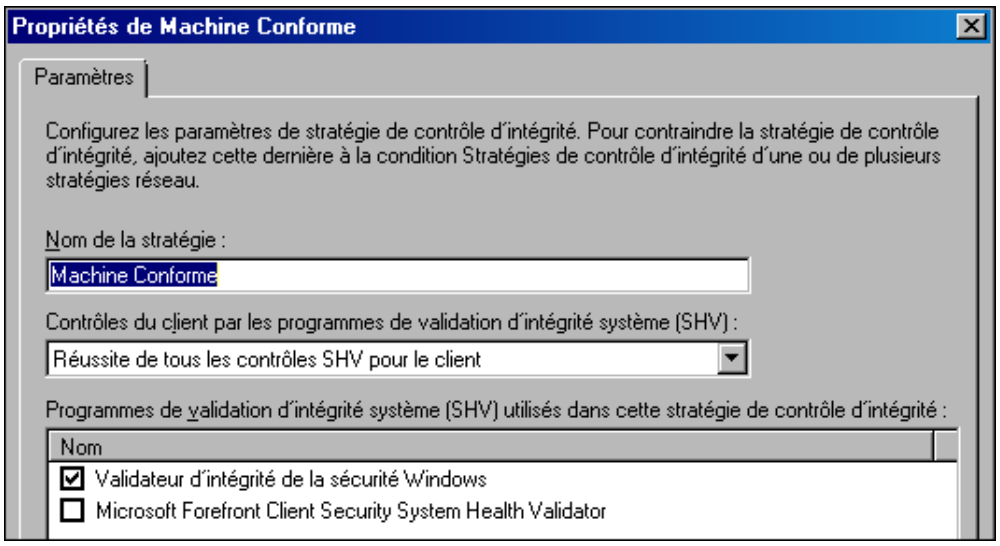


Les machines non conformes pourront se connecter aux serveurs indiqués si la **mise à jour automatique** (Remediation) est autorisée dans la stratégie réseau.

La troisième étape consiste à créer au moins deux stratégies de santé différentes.

a) Une pour les machines conformes

© ENI Editions - All rigths reserved


Propriétés de Machine Conforme
Paramètres
Configurez les paramètres de stratégie de contrôle d'intégrité. Pour contraindre la stratégie de contrôle d'intégrité, ajoutez cette dernière à la condition Stratégies de contrôle d'intégrité d'une ou de plusieurs stratégies réseau.
Nom de la stratégie :
Machine Conforme
Contrôles du client par les programmes de validation d'intégrité système (SHV) :
Réussite de tous les contrôles SHV pour le client
Programmes de validation d'intégrité système (SHV) utilisés dans cette stratégie de contrôle d'intégrité :
Nom
Validateur d'intégrité de la sécurité Windows
Microsoft Forefront Client Security System Health Validator

Seuls les validateurs activés entrent dans la règle de conformité !

b) Une pour les machines non conformes

- Sélectionnez le même validateur que pour une machine conforme, mais définissez la règle sur **Echec d'un ou de plusieurs contrôles SHV pour le client**.

La quatrième étape est la création des stratégies réseau.

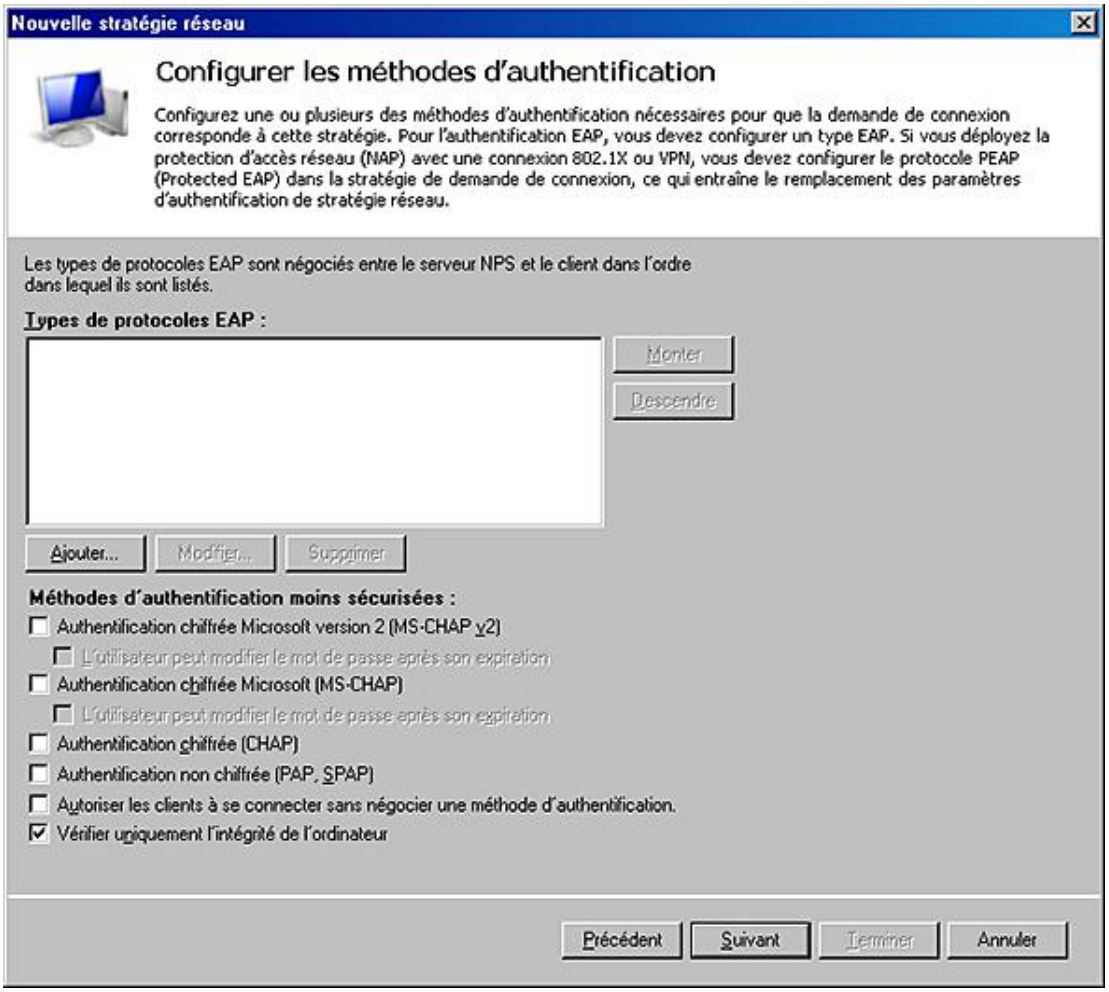
a) Création de la stratégie réseau pour les machines conformes

- Cliquez avec le bouton droit sur **Stratégies Réseau**.
- Puis choisissez **Nouveau** dans le menu.
- Nommez la stratégie **Accès complet pour les machines conformes**, laissez le type de réseau sur **Non spécifié**.

Non spécifié signifie que la stratégie sera appliquée quel que soit le type d'accès réseau utilisé.

- Sur l'écran **Spécifier les conditions**, il est impératif de préciser à qui s'applique cette stratégie, cliquez sur **Ajouter**.
- De nombreuses conditions complexes peuvent être appliquées, sélectionnez **Stratégies de contrôle d'intégrité**.
- Choisissez dans la liste proposée la stratégie **Machine Conforme**, puis passez à l'écran suivant.
- Spécifiez **Accès accordé**, ce qui est logique pour des machines conformes !
- Aucune authentification n'est requise pour ce type de quarantaine, sélectionnez donc **Vérifier uniquement l'intégrité de l'ordinateur**.

© ENI Editions - All rigths reserved


Nouvelle stratégie réseau
Configurer les méthodes d'authentification
Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.
Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.
Types de protocoles EAP :
Monter
Descendre
Ajouter...
Modifier...
Supprimer
Méthodes d'authentification moins sécurisées :
Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée Microsoft (MS-CHAP)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée (CHAP)
Authentification non chiffrée (PAP, SPAP)
Autoriser les clients à se connecter sans négocier une méthode d'authentification.
Vérifier uniquement l'intégrité de l'ordinateur
Précédent
Suivant
Terminer
Annuler

- Sur l'écran **Configurer des contraintes**, aucune valeur n'est à modifier.

- Sur l'écran **Configurer les paramètres**, il s'agit d'appliquer une configuration (modification) du client réseau. Ici, dans la section **Protection d'accès réseau**, on va **Autoriser un accès réseau complet**.

- Cliquez sur **Terminer** sur l'écran final qui résume l'ensemble de la stratégie.

b) Création de la stratégie réseau pour les machines non conformes

- Cliquez avec le bouton droit sur **Stratégies Réseau** puis choisissez **Nouveau** dans le menu.

- Nommez la stratégie **Accès complet pour les machines non conformes**, laissez le type de réseau sur **Non spécifié** comme pour les machines conformes.

- Sur l'écran **Spécifier les conditions**, il est impératif de préciser à qui s'applique cette stratégie, cliquez sur **Ajouter**.

- De nombreuses conditions complexes peuvent être appliquées, sélectionnez **Stratégies de contrôle d'intégrité**, puis choisissez dans la liste proposée la stratégie **Machine non Conforme**, puis passez à l'écran suivant.

- Spécifiez **Accès accordé**. En effet, même pour des machines non conformes, il s'agit d'une règle qui va aussi autoriser un accès mais seulement aux éléments autorisés !

- Aucune authentification n'est requise pour ce type de quarantaine, sélectionnez donc **Vérifier uniquement l'intégrité de l'ordinateur** comme pour les machines conformes.

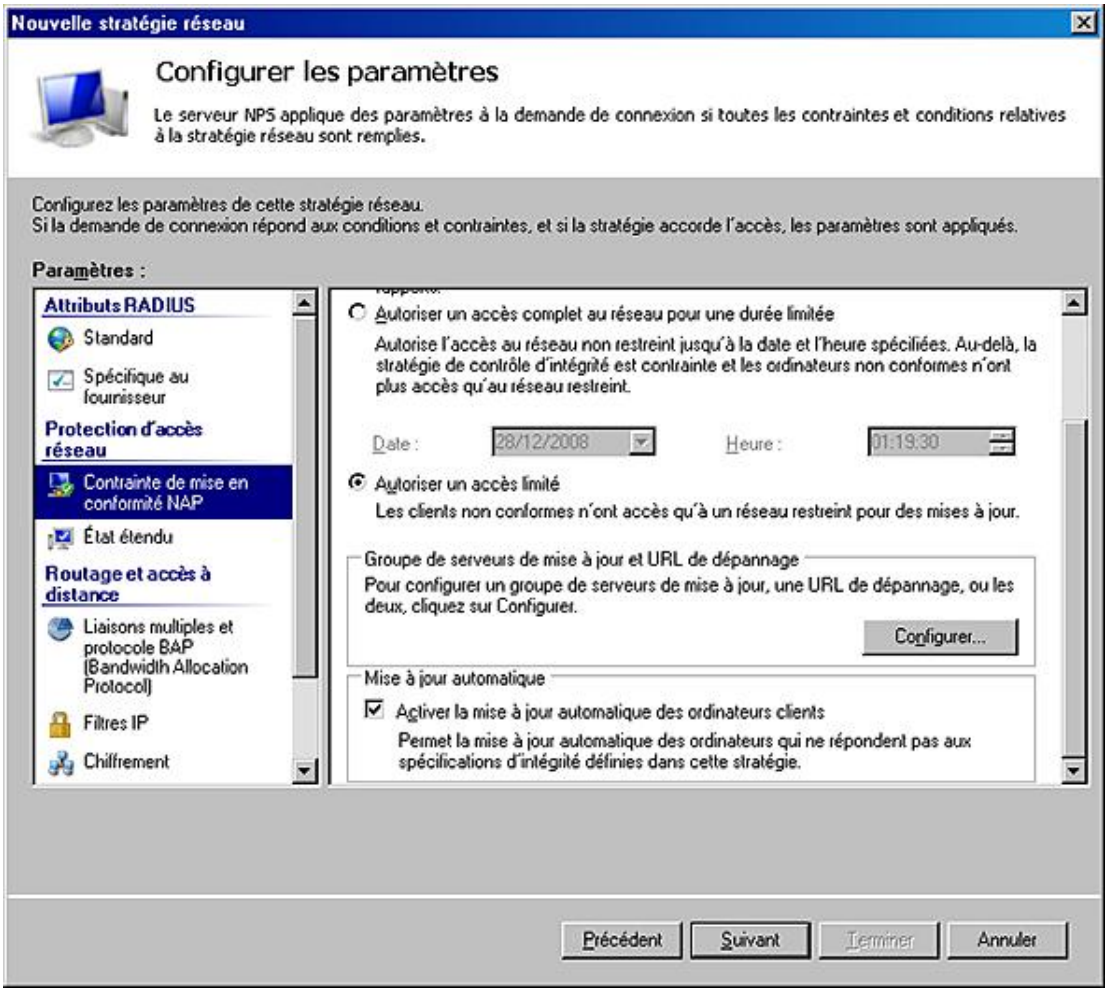
- Sur l'écran **Configurer des contraintes**, aucune valeur n'est à modifier.

© ENI Editions - All rigths reserved

- Sur l'écran **Configurer les paramètres**, il s'agit d'appliquer une configuration (modification) du client réseau. Ici, dans la section **Protection d'accès réseau**, on va **Autoriser un accès limité**.

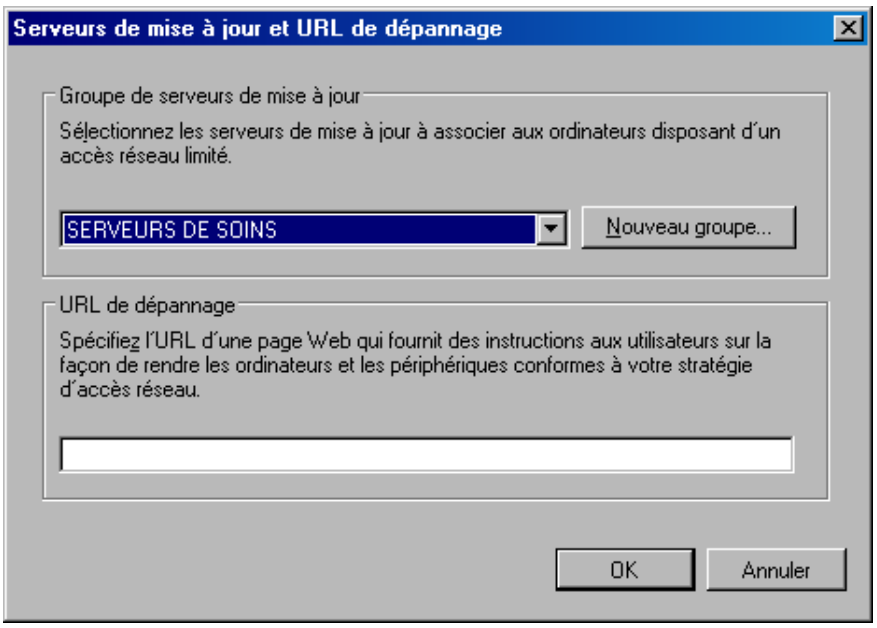
Le choix d'**autoriser un accès limité** ne doit être pris que lorsque l'on est sur des effets de sa stratégie. Il est souvent préférable d'autoriser d'abord un accès complet, d'utiliser le mode rapport pour avoir une idée de l'étendue des machines qui seraient impactées.

- Si l'on veut autoriser la remise à niveau automatique (et donc autoriser les serveurs de remediation), il faut cocher la case **Activer la mise à jour automatique des ordinateurs clients**.


Nouvelle stratégie réseau
Configurer les paramètres
Le serveur NPS applique des paramètres à la demande de connexion si toutes les contraintes et conditions relatives à la stratégie réseau sont remplies.
Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.
Paramètres :
Attributs RADIUS
Standard
Spécifique au fournisseur
Protection d'accès réseau
Contrainte de mise en conformité NAP
État étendu
Routage et accès à distance
Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
Filtres IP
Chiffrement
Autoriser un accès complet au réseau pour une durée limitée
Autorise l'accès au réseau non restreint jusqu'à la date et l'heure spécifiées. Au-delà, la stratégie de contrôle d'intégrité est contrainte et les ordinateurs non conformes n'ont plus accès qu'au réseau restreint.
Date :
28/12/2008
Heure :
01:19:30
Autoriser un accès limité
Les clients non conformes n'ont accès qu'à un réseau restreint pour des mises à jour.
Groupe de serveurs de mise à jour et URL de dépannage
Pour configurer un groupe de serveurs de mise à jour, une URL de dépannage, ou les deux, cliquez sur Configurer.
Configurer...
Mise à jour automatique
Activer la mise à jour automatique des ordinateurs clients
Permet la mise à jour automatique des ordinateurs qui ne répondent pas aux spécifications d'intégrité définies dans cette stratégie.
Précédent
Suivant
Terminer
Annuler

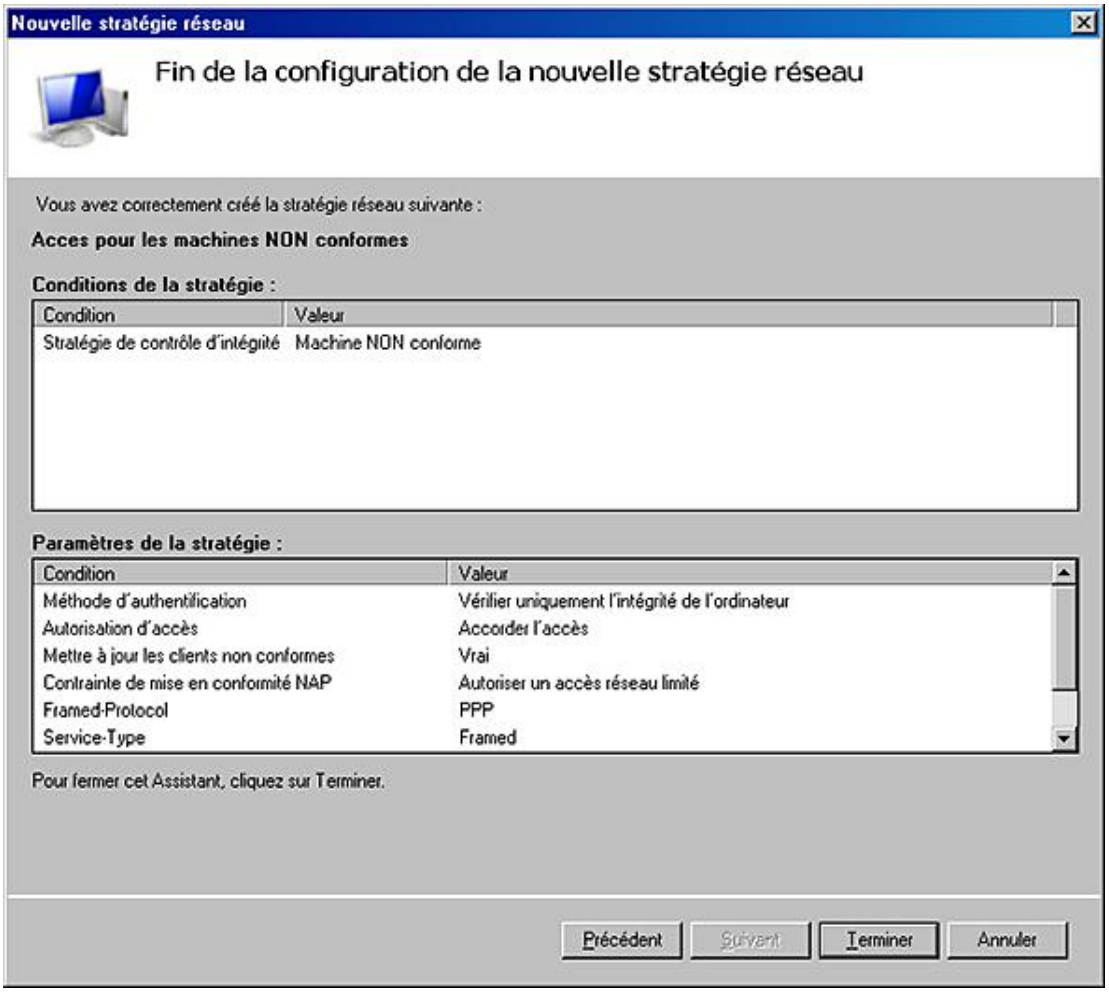
- Cliquez sur **Configurer** pour spécifier un **Groupe de serveurs de mise à jour** ainsi que l'adresse d'une page Web optionnelle d'explication pour les utilisateurs.

© ENI Editions - All rigths reserved


Serveurs de mise à jour et URL de dépannage
Groupe de serveurs de mise à jour
Sélectionnez les serveurs de mise à jour à associer aux ordinateurs disposant d'un accès réseau limité.
SERVEURS DE SOINS
Nouveau groupe...
URL de dépannage
Spécifiez l'URL d'une page Web qui fournit des instructions aux utilisateurs sur la façon de rendre les ordinateurs et les périphériques conformes à votre stratégie d'accès réseau.
OK
Annuler

Sur les clients restreints, chaque serveur indiqué dans ce groupe dispose de sa propre route avec un masque à 255.255.255.255. Assez logiquement, les autres serveurs ne sont pas accessibles.

- Cliquez sur **Terminer** sur l'écran final qui résume l'ensemble de la stratégie.



À noter que, selon la répartition des rôles sur les différents serveurs autorisés, la réparation automatique (remediation) peut parfois nécessiter un accès complet.

Le client **Agent de protection d'accès réseau** doit être actif sur les postes clients, c'est-à-dire que le service doit être en démarrage automatique !

© ENI Editions - All rigths reserved

Le Centre de sécurité doit avoir été activé, ce qui peut se faire par stratégie.

La console du client NAP (`NAPCLCFG.MSC`) permet de vérifier les contraintes mises en place.

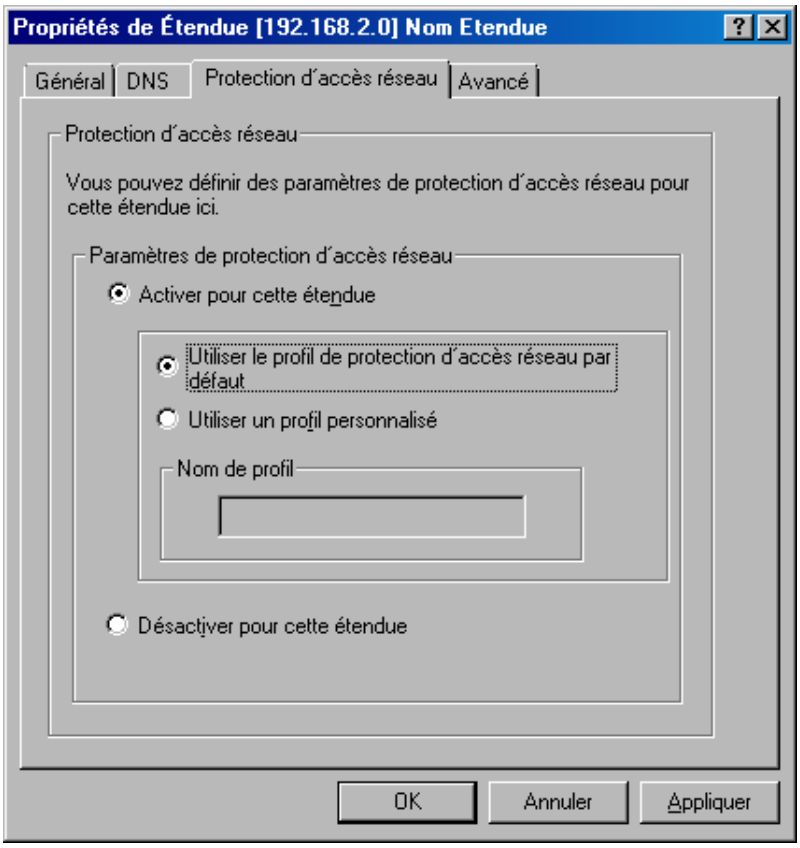
La commande `Napstat` permet de vérifier la conformité par rapports aux règles établies.

2. La mise en place de NAP via DHCP

Lorsque les préparations initiales décrites plus haut ont été réalisées, il ne reste que peu d'étapes à ajouter pour que NAP sur DHCP fonctionne.

L'étendue DHCP doit tout d'abord être activée pour utiliser la sécurité basée sur NAP.

Dans les propriétés de l'étendue, vous trouverez l'onglet **Protection d'accès réseau**.



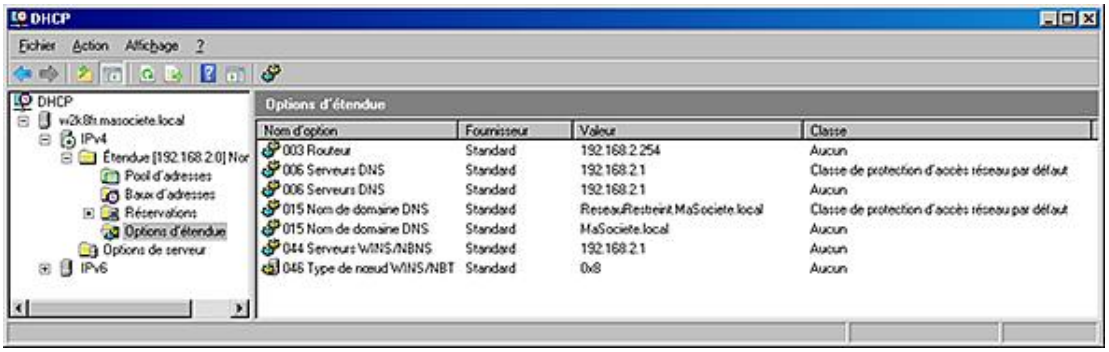
Les machines qui sont conformes aux pré-requis utilisent les options que vous avez configurées dans les **options standard DHCP** (Classe du fournisseur), pour la **Classe utilisateur par défaut**.

Le **profil de protection d'accès réseau par défaut** correspond à la classe d'utilisateur **Classe de protection d'accès réseau par défaut**. Les machines non conformes utiliseront les options définies au niveau de cette classe.

Seules les options souhaitables sont à définir, donc par exemple :

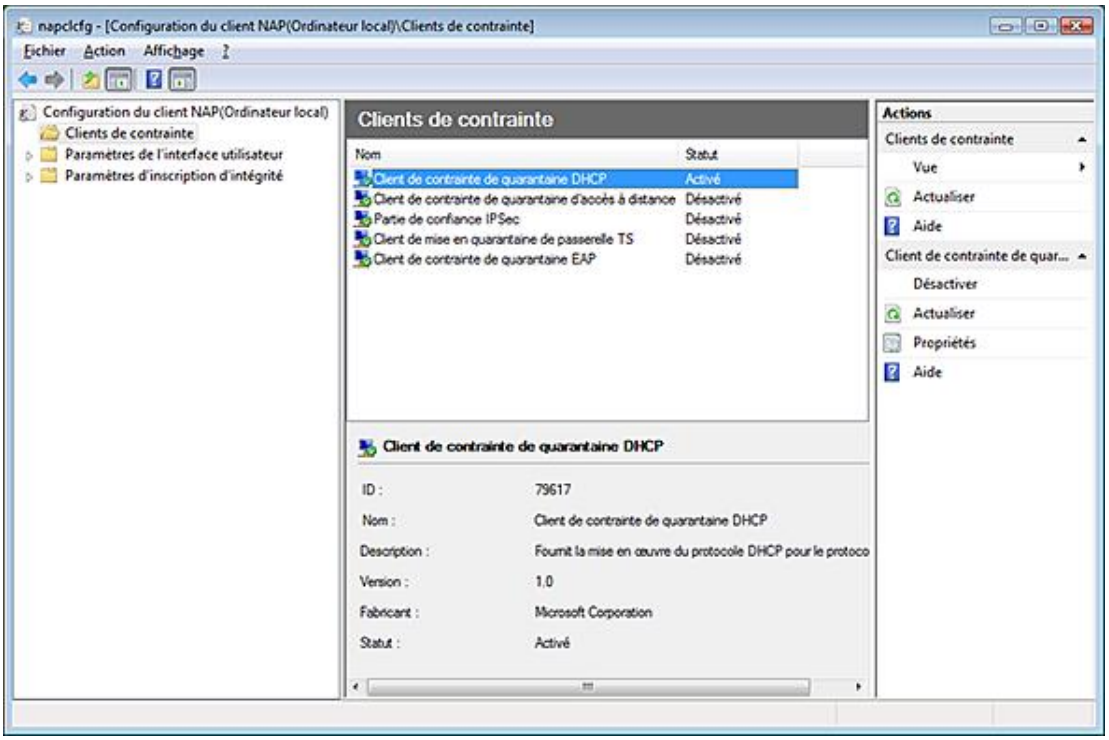
- un serveur DNS spécifique ou non permettant d'atteindre ou de résoudre certains noms ;
- une zone DNS fictive ou non mais spécifique pour identifier rapidement les machines non conformes ;
- pas de routeur pour empêcher la machine d'accéder à des parties de réseau à protéger.

© ENI Editions - All rigths reserved


DHCP
Fichier Action Affichage ?
DHCP
w2k8t.masociete.local
IPv4
Étendue [192.168.2.0] Nor
Pool d'adresses
Baux d'adresses
Réservations
Options d'étendue
Options de serveur
IPv6
Options d'étendue
Nom d'option Fournisseur Valeur Classe
003 Routeur Standard 192.168.2.254 Aucun
006 Serveurs DNS Standard 192.168.2.1 Classe de protection d'accès réseau par défaut
006 Serveurs DNS Standard 192.168.2.1 Aucun
015 Nom de domaine DNS Standard ReseauRestreint.MaSociete.local Classe de protection d'accès réseau par défaut
015 Nom de domaine DNS Standard MaSociete.local Aucun
044 Serveurs WINS/NBNS Standard 192.168.2.1 Aucun
046 Type de noeud WINS/NBT Standard 0x8 Aucun

Les options particulières apparaissent avec une classe réseau spécifique.

La stratégie de quarantaine DHCP peut maintenant être activée sur DHCP, soit par stratégie, soit directement dans l'**outil de configuration du client NAP** que l'on peut lancer par la commande `NAPCLCFG.MSC`.


napclcfg - [Configuration du client NAP(Ordinateur local)\Clients de contrainte]
Fichier Action Affichage ?
Configuration du client NAP(Ordinateur local)
Clients de contrainte
Paramètres de l'interface utilisateur
Paramètres d'inscription d'intégrité
Clients de contrainte
Nom Statut
Client de contrainte de quarantaine DHCP Activé
Client de contrainte de quarantaine d'accès à distance Désactivé
Partie de confiance IPSec Désactivé
Client de mise en quarantaine de passerelle TS Désactivé
Client de contrainte de quarantaine EAP Désactivé
Client de contrainte de quarantaine DHCP
ID : 79617
Nom : Client de contrainte de quarantaine DHCP
Description : Fournit la mise en œuvre du protocole DHCP pour le protoco
Version : 1.0
Fabricant : Microsoft Corporation
Statut : Activé
Actions
Clients de contrainte
Vue
Actualiser
Aide
Client de contrainte de quar...
Désactiver
Actualiser
Propriétés
Aide

En cas d'arrêt du service **Pare-Feu Windows**, la station ne sera plus conforme. Si la mise à jour automatique a été autorisée et que les serveurs de dépannages sont accessibles, les réparations sont effectuées immédiatement. Dans notre cas, le redémarrage immédiat du service Pare-Feu remet la station conforme et fonctionnelle.

Utilisez la commande `napstat.exe` pour vérifier le statut de conformité des stations par rapport aux stratégies mises en place. Une icône vient se placer dans la zone de notification et reste en place tant que l'on ne ferme pas l'outil.

La quarantaine réseau basée sur DHCP est la plus faible des protections possibles qui est facilement contournée par tout utilisateur disposant des droits d'administrateur local de son poste.

3. La mise en place de NAP via IPSec

Cette sécurité nécessite l'installation du service **Autorité HRA** (*Health Registration Autority*).

```
servermanagercmd -install NPAS-Health
```

L'installation d'une autorité de certification de type Entreprise est nécessaire si aucun autre système de distribution de clé (PKI) n'est en place. L'utilisation du rôle Microsoft correspondant simplifie énormément la tache. Il est fortement conseillé d'utiliser l'interface graphique pour passer par l'assistant de création du certificat racine.

Afin de limiter l'application de la quarantaine basée sur IPSec, il est prudent de créer des groupes d'ordinateurs pour chaque catégorie.

© ENI Editions - All rigths reserved

- Les ordinateurs clients de NAP IPSec : c'est-à-dire toutes les stations qui doivent se conformer aux règles de sécurité.

- Les serveurs dits de frontière (**Boundary**) qui reçoivent automatiquement un certificat de **santé** et qui servent à l'authentification des clients. Les contrôleurs de domaine, les serveurs DNS et les serveurs de **réparation** (Remediation) doivent faire partie de ce groupe.

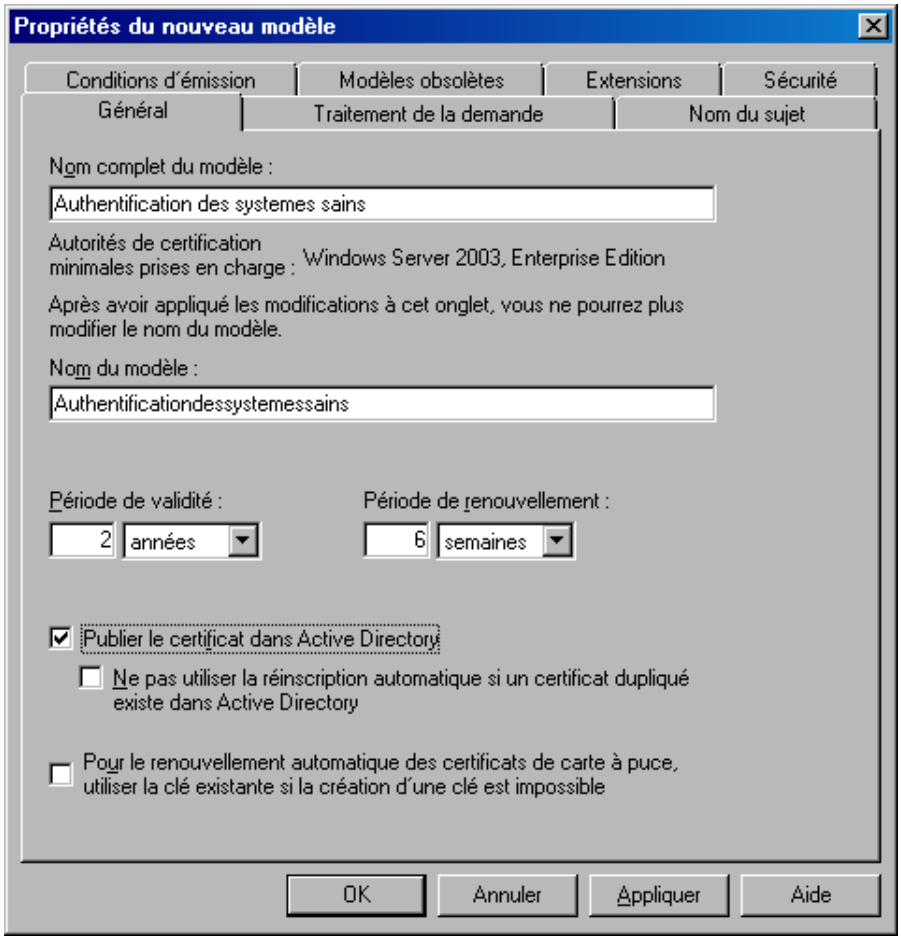
- Les ordinateurs protégés par NAP IPSec : ceux-ci reçoivent aussi automatiquement un certificat et n'autoriseront la connexion que des machines authentifiées.

Chaque machine (stations ou serveurs) doit pouvoir recevoir un certificat. Or, le certificat transmis aux stations par défaut ne contient pas la stratégie d'authentification adéquate.

- Créez un nouveau certificat **Authentification de station de travail** en dupliquant le modèle existant à partir de la **console des Modèles de Certificats** que l'on peut obtenir directement par la commande `certtmpl.msc`.

- Lors de la duplication, choisissez la compatibilité Windows 2003 ou Windows 2008. Dans tous les cas, une version Enterprise est nécessaire pour que la distribution des certificats soit automatique.

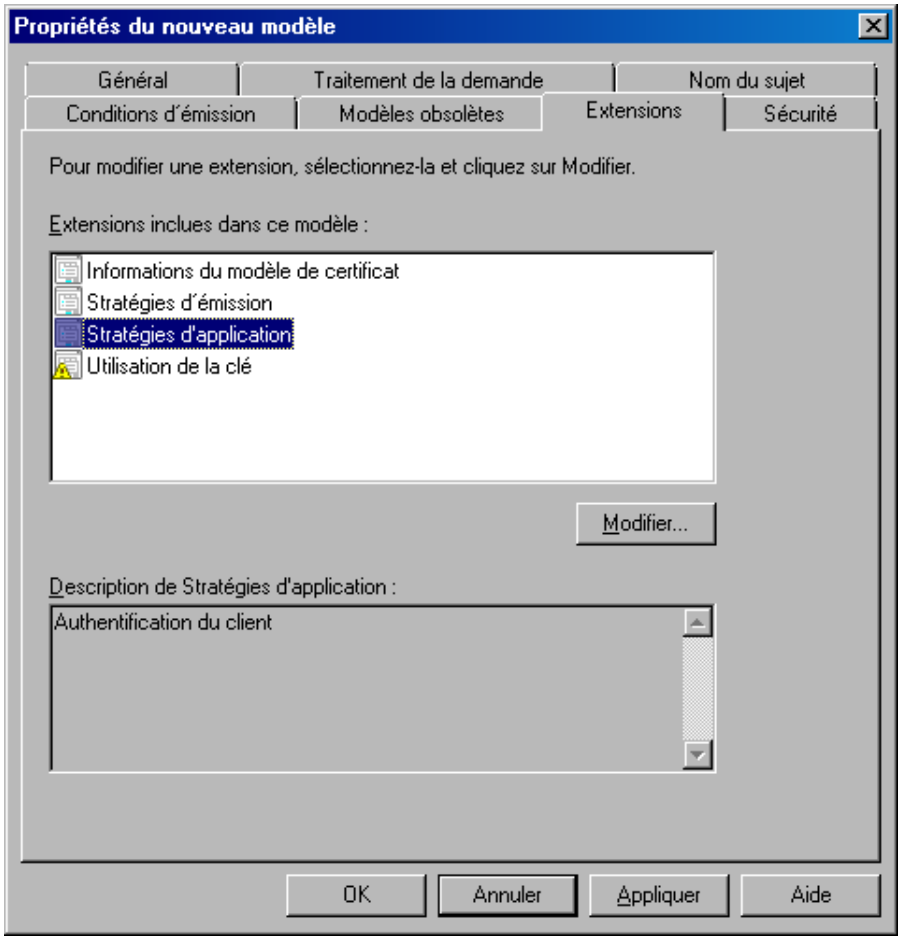
- Nommez le certificat, modifiez la période de validité et publiez le certificat dans Active Directory.


Propriétés du nouveau modèle
Conditions d'émission
Modèles obsolètes
Extensions
Sécurité
Général
Traitement de la demande
Nom du sujet
Nom complet du modèle :
Authentification des systemes sains
Autorités de certification minimales prises en charge :
Windows Server 2003, Enterprise Edition
Après avoir appliqué les modifications à cet onglet, vous ne pourrez plus modifier le nom du modèle.
Nom du modèle :
Authentificationdessystemessains
Période de validité :
2
années
Période de renouvellement :
6
semaines
Publier le certificat dans Active Directory
Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory
Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création d'une clé est impossible
OK
Annuler
Appliquer
Aide

Les serveurs impliqués dans la validation ont effectivement un certificat validé pour deux ans. En revanche, les ordinateurs qui demanderont la validation n'obtiendront qu'un certificat d'une durée de vie de quatre heures.

- Dans l'onglet **Extensions**, sélectionnez **Stratégies d'application**, et ajoutez la stratégie **Authentification** de l'Agent SHA (*System Health*).

© ENI Editions - All rigths reserved



- Au niveau de l'onglet **Sécurité**, ajoutez les groupes des serveurs de type frontière et des serveurs Protégés, et donnez les droits **Inscrire** et **Inscription automatique**.

- Dans la console **Autorité de Certification**, sur le conteneur des modèles de certificats, utilisez le bouton droit et choisissez **Modèle de certificats à délivrer**, puis le modèle **Authentification des systèmes sains**.

- Comme la validation des clients nécessitera régulièrement des certificats de **bonne santé**, il est important de vérifier que le module de stratégie (sur le certificat de la racine) soit configuré sur **Emettre automatiquement le certificat**.

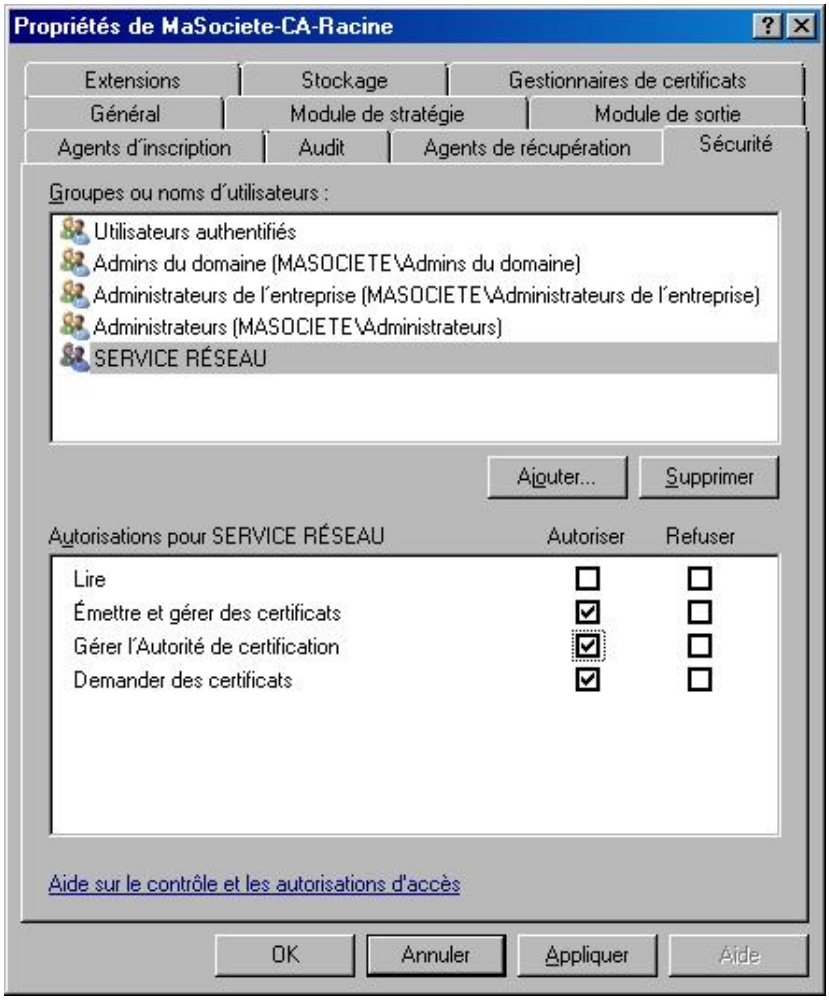
- Les clients doivent être configurés pour demander automatiquement les certificats. Dans l'outil GPMC (Gestion de Stratégie de Groupe), configurez la **demande automatique de certificats dans la Default Domain Policy**.

- Utilisez le bouton droit dans **configuration ordinateurs**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégie de clé publique**, **Paramètres de demande automatique de certificats**, sur la stratégie **Client des services de certificats - Inscription automatique**.

© ENI Editions - All rigths reserved

Propriétés de Client des services de certificats - Inscription a...
Définition des paramètres de stratégie
Inscrire automatiquement l'utilisateur et les certificats d'ordinateur
Modèle de configuration :
Activé
Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués
Mettre à jour les certificats qui utilisent les modèles de certificats
Notification d'expiration
Afficher les notifications d'expiration si le pourcentage de durée de vie restante du certificat atteint
10
%
Informations sur la gestion automatique des certificats
OK
Annuler
Appliquer

Le compte **SERVICE RESEAU** (si le CA et le HRA sont sur la même machine) ou l'ordinateur sur lequel est installé le système de validation (HRA) doit obtenir les droits suivants :



© ENI Editions - All rigths reserved

La commande suivante permet au système validateur de demander des certificats avec une durée de vie différente de la validité de deux ans définie et imposée dans le modèle.

```
certutil -setreg policy\editflags +EditF_attributeEndDate
```

La configuration du système de validation (HRA).

- Créez une console MMC et ajoutez le composant **Autorité HRA (Health Registration Autority)**.
- Ajoutez l'autorité de certification à partir de AD.
- Modifiez les propriétés de l'autorité de certification, notamment pour valider l'autorité de certification de l'entreprise, et les modèles de certificats à utiliser.

Propriétés des autorités de certification
Paramètres
Nombre de minutes entre deux demandes quand un serveur est identifié comme indisponible
5
Les certificats approuvés par cette autorité HRA (Health Registration Authority) seront valides pour :
4
Heures
Utiliser l'autorité de certification autonome
Activer les OID des stratégies
Utiliser une autorité de certification d'entreprise
Modèle de certificat authentifié conforme :
Authentificationdessystèmessains
Modèle de certificat anonyme conforme :
Authentificationdessystèmessains
OK
Annuler
Appliquer

Dans l'outil d'administration NPS, la réparation automatique doit être désactivée.

Sur le poste client, pour activer IPSec sur XP SP3, il est nécessaire de passer par la ligne de commande suivante :

```
netsh nap client set enforcement ID =79619
```

Chaque contrainte (Enforcement) dispose d'un identifiant spécifique :

- DHCP = 79617
- RAS = 79618
- IPSec = 79619
- TS Gateway = 79621
- EAP = 79623

À noter que si l'ordinateur n'est plus conforme, le certificat reçu sera invalidé immédiatement sans attendre les quatre heures !

© ENI Editions - All rigths reserved

Pour le moment, aucune restriction n'est apportée sauf le fait de disposer d'un certificat. Ces restrictions sont apportées par trois stratégies basées sur les groupes de sécurité créés au départ.

Ces stratégies peuvent être définies à la racine du domaine puisqu'un filtrage basé sur les groupes de sécurité sera mis en place.

Les serveurs de frontière doivent demander mais ne pas imposer de certificats de santé. Les serveurs protégés et les postes clients doivent imposer des certificats, néanmoins, des stratégies différentes sont préférables afin d'ajouter des configurations spécifiques pour les clients (URL de configuration HRA).

Voici la stratégie à mettre en place sur les serveurs de frontière (Boundary) :

- Dans **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - LDAP ...** créez une nouvelle règle de sécurité dans **Règles de sécurité de connexion**, choisissez **Isolation** puis **Demander l'authentification des connexions entrantes et sortantes**, puis l'authentification par **Certificat d'ordinateur**.
- Indiquez votre autorité de certification du domaine, et cochez la case **N'accepter que les certificats d'intégrité**.
- Laissez cochés tous les profils qui s'appliquent **Domaine**, **Privée**, **Publiques**.
- Nommez cette règle **REGLE NAP IPSEC Frontière**.
- Sur l'onglet **Etendue de la stratégie**, ajoutez un filtrage de sécurité pour le groupe **Serveurs IPSEC de Frontière**.

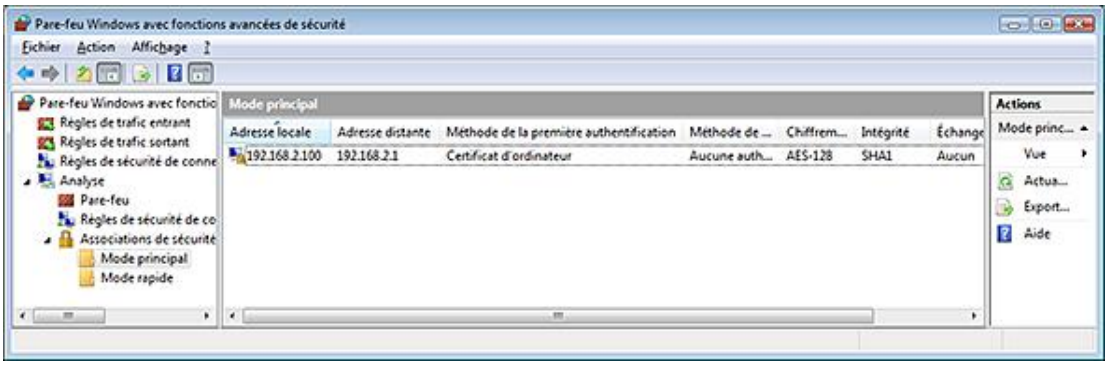
Voici la nouvelle stratégie à mettre en place sur les clients :

- Dans **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - Pare-feu Windows avec fonctions avancées de sécurité - LDAP...** créez une **nouvelle règle** de sécurité dans **Règles de sécurité de connexion**, choisissez **Isolation**, puis **Imposer l'authentification des connexions entrantes et demander l'authentification des connexions sortantes**, puis l'authentification par **Certificat d'ordinateur**.
- Indiquez votre autorité de certification du domaine, et cochez la case **N'accepter que les certificats d'intégrité**.
- Laissez cochés tous les profils qui s'appliquent **Domaine**, **Privée**, **Publiques**.
- Nommez cette règle **REGLE NAP IPSEC Client**.
- Sur l'onglet **Etendue** de la stratégie, ajoutez un filtrage de sécurité pour le groupe **Clients IPSEC**.

Une stratégie identique sera créée pour les serveurs à protéger.

En utilisant l'instruction `ping -t` vers un serveur de frontière ou un serveur protégé, il sera possible de vérifier l'utilisation de l'authentification par certificat avec l'outil **Pare-feu Windows avec fonctions avancées de sécurité**.

Une association de sécurité basée sur les certificats sera utilisée pour la communication.



Bien sûr, ceci n'est qu'une possibilité de mise en place de la sécurité basée sur la quarantaine par IPSec ! Il est fort prudent de maquetter l'ensemble du réseau avant de la mettre en place sur le réseau de production.

© ENI Editions - All rigths reserved

4. La mise en place de NAP sur 802.1x

802.1X était jusqu'à présent principalement réservé aux points d'accès sans fil.

Maintenant, NAP permet aussi d'utiliser plus facilement cette authentification directement sur le réseau local. Cette mise en place suppose l'utilisation de radius pour relayer la demande, et l'affectation d'un VLAN spécifique grâce à un switch acceptant les VLAN.

Trois éléments sont nécessaires :

- un serveur d'authentification ;
- un agent authentificateur (Switch ou Point d'accès Sans-fil) ;
- le demandeur.

Le client demandeur utilise le protocole EAP (EAP over Lan) pour envoyer la demande à l'agent d'authentification (Pass-Through). L'agent Pass-Through peut alors interroger un serveur RADIUS pour valider ou non la connexion.

Sous Windows 2008, le serveur NPS remplace la technologie IAS mais continue à utiliser le protocole RADIUS pour communiquer. Si les clients ne sont pas conformes avec la sécurité demandée, un réseau restreint utilisant un VLAN spécifique ou un filtrage IP leur est affecté.

a) La configuration du switch (ou point d'accès) :

Voici la configuration des différents VLAN à réaliser sur le switch (ou point d'accès):

- VLAN ID 1 = est le VLAN par défaut ;
- VLAN ID 2 = pour les machines non conformes ;
- VLAN ID 3 = pour les machines conformes.

Le routage InterVLAN doit être désactivé entre le VLAN 2 et le VLAN 3.

Les ports utilisés pour connecter le serveur NPS et les contrôleurs de domaine doivent être configurés pour ne pas imposer l'authentification 802.1X. Toutes les demandes d'authentification et d'autorisation du switch doivent être redirigées vers le serveur NPS.

b) Dans la forêt Active Directory, une autorité racine de certification de type Entreprise est aussi nécessaire. Le serveur NPS doit avoir reçu un certificat d'ordinateur et le certificat racine devrait être ajouté parmi les autorités principales de confiance sur toutes les machines.

Un groupe de sécurité spécifique appelé **Clients NAP 802.1X** pour les clients NAP 802.1X peut être créé afin de restreindre l'application des stratégies aux machines ajoutées à ce groupe.

La plupart des éléments (Contrôleur de domaine, Serveur NPS, Autorité de certification, Gestion de stratégies de groupes) peuvent être installés sur une même machine, ce qui simplifiera la configuration de test. Si les systèmes précédents de quarantaine ont été testés, tous les éléments nécessaires sont déjà en place. En revanche, il sera préférable, dans un premier temps, de supprimer ou désactiver les stratégies de groupe et les stratégies réseau déjà configurées.

c) Configurez le serveur NPS en tant que serveur de stratégie de **santé** (Health Policy Server) :

Le plus simple est d'utiliser l'assistant de configuration de NAP !

À partir de la racine (NPS Local) :

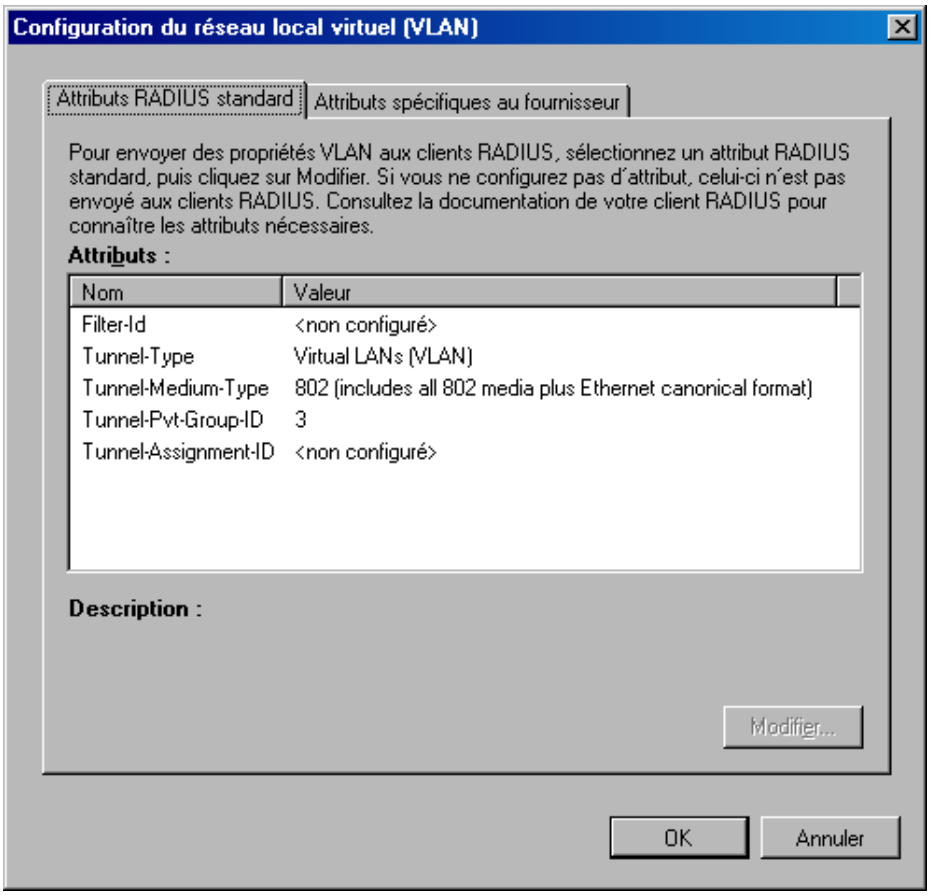
- Cliquez sur **Configurer la protection d'accès réseau (NAP)** dans la partie **Configuration standard**.
- Dans **Méthode de connexion réseau**, sélectionnez **IEE 802.1X (câblé)**.
- Dans les **Clients RADIUS**, ajoutez l'adresse IP du ou des switch radius, ainsi que la phrase secrète qui sera utilisée par le client.
- Sur l'écran **Groupes d'ordinateurs et d'utilisateurs**, ne rien indiquer.
- Pour la méthode d'authentification, cliquez sur **Choisir** et sélectionnez le certificat (valide) émis pour le serveur

© ENI Editions - All rigths reserved

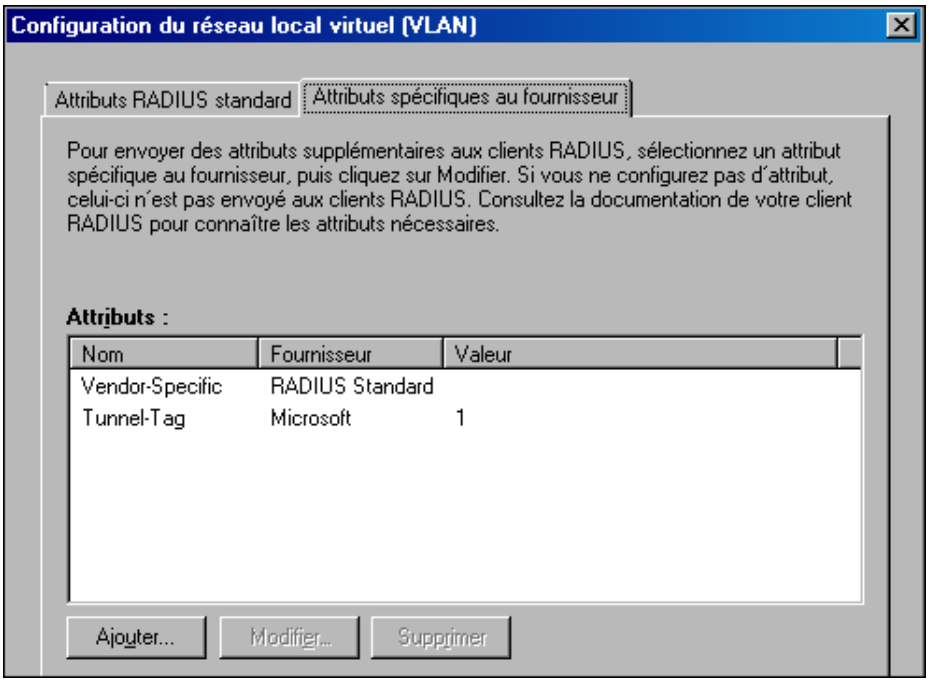
hébergeant NPS et validez le mode **PEAP-MS-CHAP v2**.

Il faut ensuite configurer les deux réseaux locaux virtuels (VLAN) de la manière suivante en cliquant sur **Configurer** :

d) Le VLAN du réseau de l'organisation à obtenir en modifiant chaque attribut standard :

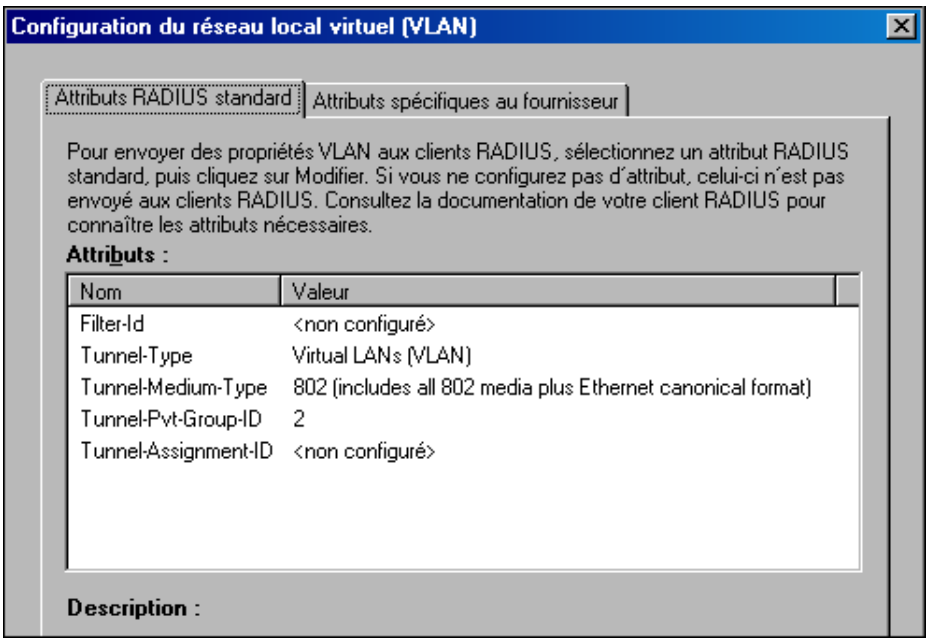

Configuration du réseau local virtuel (VLAN)
Attributs RADIUS standard
Attributs spécifiques au fournisseur
Pour envoyer des propriétés VLAN aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Filter-Id
<non configuré>
Tunnel-Type
Virtual LANs (VLAN)
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID
3
Tunnel-Assignment-ID
<non configuré>
Description :
Modifier...
OK
Annuler

Un attribut (tag) spécifique à Microsoft doit être ajouté :


Configuration du réseau local virtuel (VLAN)
Attributs RADIUS standard
Attributs spécifiques au fournisseur
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Fournisseur
Valeur
Vendor-Specific
RADIUS Standard
Tunnel-Tag
Microsoft
1
Ajouter...
Modifier...
Supprimer

Le VLAN du réseau restreint :

© ENI Editions - All rigths reserved


Configuration du réseau local virtuel (VLAN)
Attributs RADIUS standard
Attributs spécifiques au fournisseur
Pour envoyer des propriétés VLAN aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Filter-Id
<non configuré>
Tunnel-Type
Virtual LANs (VLAN)
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID
2
Tunnel-Assignment-ID
<non configuré>
Description :

L'attribut spécifique **Tunnel-Tag** de Microsoft doit aussi être positionné sur **1**.

- Dans **Définir la stratégie de contrôle d'intégrité NAP**, sélectionnez le système de validation souhaité, c'est-à-dire le **Validateur d'intégrité de la sécurité Windows**, dans notre cas.

- Par défaut, l'accès réseau complet n'est pas accordé aux clients non conformes.

- Toutes les stratégies sont créées sur l'écran final en cliquant sur **Terminer**.

e) Après configuration par l'assistant, il est intéressant de revérifier chaque paramètre.

  - Pour la réalisation des tests, le validateur d'intégrité de la sécurité Windows est configuré pour ne vérifier que le démarrage du service pare-feu.

  - Les stratégies de contrôles d'intégrité (définir les validateurs à utiliser).

  - Les stratégies de demande de connexion (vérifiez l'ordre d'exécution, notez que la stratégie NAP 802.1X ne s'applique qu'aux connexions de type **ETHERNET**).

  - Les stratégies réseau, et en particulier la stratégie **NAP 802.1X (câblé) Non Compatible NAP**.

En effet, lors de la mise en place de stratégies sur le réseau, il est primordial de traiter l'existence des machines Unix, Linux, Mac ou autres qui ne seraient pas compatibles NAP. Ces machines doivent continuer à fonctionner et communiquer sur le réseau, soit par des exclusions, soit par des règles spécifiques !

f) Pour que les clients NAP soient déclarés **conformes**, il est nécessaire que les clients aient la configuration adaptée. Pour les machines intégrées au domaine, il est logique d'utiliser les stratégies de groupes pour forcer la bonne configuration.

Voici les points importants de cette stratégie :

- Démarrez automatiquement le service **Agent de protection d'accès réseau**.

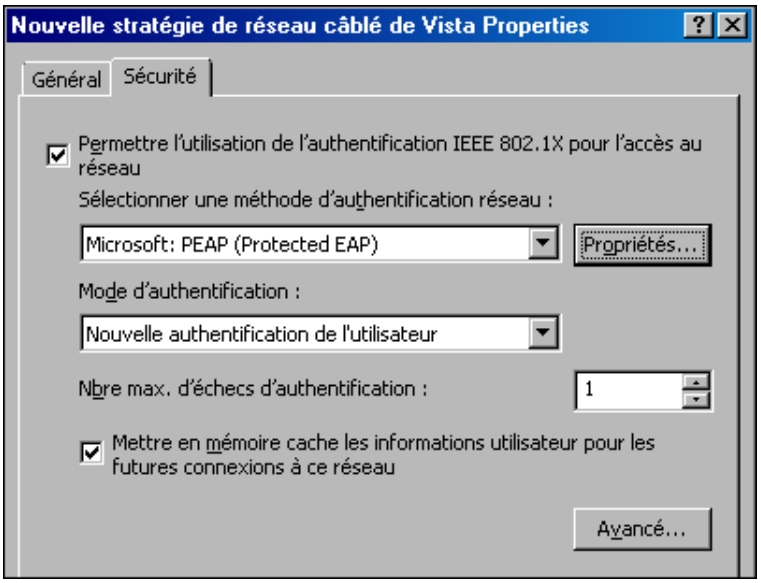
- Démarrez automatiquement le service **Configuration automatique de réseau câblé**.

- Activez le **Client de contrainte de quarantaine EAP** dans la section **Paramètres Windows - Paramètres de sécurité - Network Access Protection - Configuration du client NAP - Clients de contrainte**.

- Activez le **Centre de sécurité (Ordinateurs appartenant à un domaine)**.

© ENI Editions - All rigths reserved

- Dans **Stratégies de réseau filaire (IEEE 802.3)**, créez une stratégie de réseau câblé ayant les paramètres suivants :


Nouvelle stratégie de réseau câblé de Vista Properties
Général
Sécurité
Permettre l'utilisation de l'authentification IEEE 802.1X pour l'accès au réseau
Sélectionner une méthode d'authentification réseau :
Microsoft: PEAP (Protected EAP)
Propriétés...
Mode d'authentification :
Nouvelle authentification de l'utilisateur
Nbre max. d'échecs d'authentification :
1
Mettre en mémoire cache les informations utilisateur pour les futures connexions à ce réseau
Avancé...

- Cliquez sur **Propriétés** et laissez la case **Valider le certificat du serveur** cochée, ainsi que la méthode d'authentification **EAP-MSCHAP v2** par défaut.

- Décochez la case **Activer la reconnexion rapide**.

- Cochez la case **Activer les tests de quarantaine**.

- Si l'on veut restreindre cette stratégie à un groupe d'ordinateurs précis, retirez le groupe **Utilisateurs authentifiés** dans la partie **Filtrage de sécurité** et ajoutez le groupe **Clients NAP 802.1X** créé en début de procédure.

Attention, n'oubliez pas d'intégrer les clients dans ce groupe !

À noter que les paramètres peuvent aussi être configurés manuellement sur la station, à condition de démarrer manuellement tous les services indiqués dans la stratégie.

5. Conclusion

Voici les résultats obtenus avec ces différents types de quarantaine.

Règles	Client correct	Client incorrect
DHCP	Adresse IP complète et accès complet	Des routes restreintes
802.1X	Accès complet	Accès au VLAN restreint ou aux ports autorisés
IPSec	Communication avec tout pair de confiance	Les pairs de confiance Rejettent les connexions des systèmes non surs

La meilleure sécurité sera obtenue par 802.1X, suivi de près par IPSec, DHCP pouvant être facilement contourné. Dans tous les cas, la quarantaine n'est pas une sécurité absolue mais améliore fortement la sécurité globale en favorisant la remise à niveau de l'ensemble du réseau.

D'autres types de quarantaine existent, mais ne s'appliquent pas à la totalité du réseau : il s'agit de la quarantaine VPN, Accès Distant et TS.

Une des seules contraintes à l'utilisation de la quarantaine consiste à utiliser Windows XP SP3 ou Vista, et de démarrer les services de protection réseau nécessaires. Néanmoins, il est important de noter que de nombreux fournisseurs proposent des produits compatibles NAP et notamment qu'il existe des clients NAP pour Linux et Mac.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre est dédié au déploiement des serveurs et postes de travail. Posséder un socle d'installation automatisé est un gain de productivité et de qualité très notable. L'installation de serveurs a peu de valeur ajoutée mais doit toujours être faite de la même façon, avec les mêmes versions de composants, afin d'avoir une cohérence entre tous les systèmes. Un déploiement comprend au minimum le système d'exploitation, mais aussi généralement l'ensemble des pilotes, utilitaires systèmes, voir même l'ensemble des applications nécessaires.

L'automatisation de ce processus prend encore plus de sens avec la virtualisation, et les environnements « à la demande ». La préparation de ce déploiement a une part très importante dans la réussite de votre projet. La technique n'étant pas une difficulté ici, il n'y a aucune raison de s'en priver !

© ENI Editions - All rigths reserved

Préparer son déploiement en choisissant bien sa stratégie

La préparation est la phase critique du projet. Afin de ne rien oublier tout en accélérant votre déploiement, Microsoft propose différents outils adaptés à votre contexte. À la fin de cette partie, vous aurez déterminé le périmètre, le type de licence et d'édition de Windows, le vecteur de déploiement ainsi que l'infrastructure à mettre en œuvre pour y parvenir.

1. Définir le périmètre

Comme pour tout projet, le périmètre est ici un élément clé. Vous devriez définir ce qui est « obligatoire » de ce qui est « facultatif/optionnel ». Afin d'alimenter votre réflexion, voici une liste d'éléments pouvant être intégrés dans votre projet :

- Seulement les serveurs ou aussi les postes clients ?
- Quelles versions et éditions de Windows sont à inclure ?
- Faut-il gérer plusieurs langues ?
- Quelle nomenclature adopter pour les systèmes ainsi déployés ?
- Qui va déployer ces images ? La mise en œuvre doit-elle être entièrement automatisée ?
- Quels matériels (et donc pilotes) sont à inclure ?
- Est-ce que des mises à jour Windows doivent/peuvent déjà être présentes post déploiement ?
- Quels outils ou applications font partis du tronc commun et peuvent donc être présents post déploiement ? Pouvez-vous faire une installation générique et automatisée de ces applications ?
- Faut-il créer plusieurs images de déploiement avec différentes options ou une seule image suffit ? Faut-il une image spécifique pour vos environnements virtuels ?
- Est-ce que toutes les machines à déployer sont sur le réseau local et dans le domaine ? Faut-il pouvoir installer une image depuis un DVD ?
- Utilisez-vous déjà SCCM 2007 (*System Center Configuration Manager 2007*) ?
- Comment allez-vous gérer les licences associées à vos systèmes d'exploitation ? Utilisez-vous des licences en volume ?

La réponse à l'ensemble de ces questions couvre déjà une grande partie du périmètre. Les choix qui impactent le plus un projet de déploiement sont :

- l'utilisation de SCCM 2007, qui permet un déploiement « zero touch » ;
- l'intégration d'applications dans l'image ;
- le choix du mode de transport pour le déploiement (réseau ou autre).

Le fait d'inclure plus ou moins de types de matériels n'a qu'un impact sur le temps nécessaire afin d'inclure les pilotes adéquats. Vous aurez remarqué l'emploi du terme « image » pour désigner la méthode de déploiement. Il s'agit en effet de construire un modèle de serveur, que l'on va par exemple capturer sous forme d'image, et rendre générique. Cela rend l'intégration d'applications dans le déploiement très simple, du moment que leur installation est générique. Cette image peut ensuite être déployée par divers moyens, tel que le réseau ou un DVD.

© ENI Editions - All rigths reserved

2. Gestion des licences

Contrairement aux versions précédentes de Windows, Windows Server 2008 et Windows Vista introduisent un service de gestion des licences en volume : KMS (*Key Management Service*). Il s'agit d'un service d'infrastructure à mettre en place sur votre réseau, afin de gérer les licences de vos serveurs et stations de travail. Si vous ne mettez pas en place ce service, chaque machine devra se connecter individuellement à Microsoft via Internet pour être activée. L'activation via le service KMS permet de ne pas avoir à contacter Microsoft pour activer Windows, et cette activation est valable 6 mois. Passée cette période, le système doit être de nouveau activé pour une période de 6 mois en se connectant à votre réseau. KMS peut être implémenté dès que vous avez au moins 25 licences Windows Vista ou 5 Windows Server 2008.

Afin de simplifier le type de licence à acheter, Microsoft a créé des groupes de produits qui ouvrent différentes versions et éditions. Les groupes sont hiérarchiques. Un groupe donne droit à lui-même ainsi que tous les groupes de niveaux inférieurs. Les groupes sont les suivants :

- Groupe Serveur C, qui couvre :
    - Windows Server 2008 Datacenter.
    - Windows Server 2008 Datacenter sans Hyper-V.
    - Windows Server 2008 pour Itanium.
- Groupe Serveur B, qui couvre :
    - Windows Server 2008 Standard.
    - Windows Server 2008 Standard sans Hyper-V.
    - Windows Server 2008 Enterprise.
    - Windows Server 2008 Enterprise sans Hyper-V.
- Groupe Serveur A, qui couvre :
    - Windows Web Server 2008.
- Groupe « Licence cliente en volume », qui couvre :
    - Windows Vista Business.
    - Windows Vista Entreprise.

Le groupe A couvre lui-même et les licences clientes en volumes. Le groupe B couvre lui-même, le groupe A et les licences clientes. Le groupe C couvre lui-même et tous les autres groupes.

L'installation de KMS est aussi simple que d'entrer la clé KMS, car le service Windows associé est déjà installé et actif par défaut (il s'agit du service **Licence du logiciel**) :

```
cscript C:\windows\system32\slmgr.vbs /ipk cléKMS
```

Le serveur doit ensuite valider cette clé auprès de Microsoft. Ce processus n'a lieu qu'une fois par ajout de clés. Si le serveur a un accès à Internet :

```
cscript C:\windows\system32\slmgr.vbs -ato
```

Dans le cas contraire, vous pouvez faire l'activation par téléphone en exécutant la commande `slui.exe 4`.

Pour détecter le serveur KMS, Windows utilise le DNS, une ressource SRV en particulier. Si les mises à jour DNS dynamiques sont autorisées, le service crée automatiquement les enregistrements DNS adéquats. Si votre environnement ne les autorise pas, vous pouvez configurer KMS pour qu'il n'essaie plus de créer la ressource SRV en exécutant :

© ENI Editions - All rigths reserved

```
cscript %systemroot%\system32\slmgr.vbs /cdns
```

La ressource SRV peut alors être créée manuellement avec les paramètres suivants :

- Service : _VLMCS
- Protocole : _TCP
- Port : 1688
- Hôte offrant le service : FQDN de l'hôte

Si le service DNS n'est pas disponible depuis un client, vous pouvez spécifier manuellement l'adresse IP du serveur KMS à utiliser avec la commande :

```
cscript %systemroot%\system32\slmgr.vbs /skms X.X.X.X:1688
```

Si un firewall est en place entre les machines à activer et le serveur KMS, le port TCP 1688 (par défaut) doit être ouvert (à l'initiative du client seulement). Si vous souhaitez changer le port TCP, il faut modifier la clé suivante à la fois sur le serveur KMS et les clients :

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL
```

Nom : `KeyManagementServicePort`

Type : `REG_SZ`

Valeur : XXXX (valeur représentant le nouveau port TCP en écoute)

Pour les environnements de tests, maquettes, temporaires, vous pouvez profiter de la période de grâce de Windows, qui peut être réinitialisée si besoin. La durée de la période de grâce et le nombre de réinitialisations dépendent de la version et de l'édition de Windows :

- Windows Vista : 30 jours de grâce, 3 réinitialisations
- Windows Vista Entreprise : 30 jours de grâce, 5 réinitialisations
- Windows Server 2008 : 60 jours de grâce, 3 réinitialisations

Si ces environnements sont respectivement reconstruits plus souvent que les 90, 150 et 180 jours, vous n'avez pas besoin d'activer Windows. À l'installation, ni Windows Vista ni Windows Server 2008 ne demandent de numéro de licence, ce qui permet d'être en période de grâce sans fournir de numéro de licence. Si le service KMS est hébergé sur une machine virtuelle, cette dernière ne doit pas être déplacée sur un autre serveur physique. Ce type de changement est en effet détecté par KMS, qui nécessite alors de nouveau une activation auprès de Microsoft avant de pouvoir fournir de nouvelles licences.

Pour connaître le nombre de licences actuellement utilisé sur votre KMS, vous pouvez exécuter la commande suivante :

```
cscript %systemroot%\system32\slmgr.vbs /dli
```

Si vous ne souhaitez pas utiliser KMS mais tout de même activer en masse vos Windows, vous pouvez utiliser VAMT (*Volume Activation Management Tool*). Il est téléchargeable directement depuis MDT 2008, dans le nœud **Components**.

3. Choix de l'édition et du type d'installation

Au-delà de l'impact sur la gestion des licences, chaque paire édition/type d'installation (complète ou minimale) va nécessiter une nouvelle image de déploiement. Le choix de l'édition dépend de plusieurs critères :

- les rôles nécessaires ;
- les fonctionnalités nécessaires ;

© ENI Editions - All rigths reserved

- les ressources matérielles à utiliser ;
- l'homogénéité de vos systèmes dans votre infrastructure afin d'avoir une édition couvrant le maximum de vos besoins ;
- une installation de type Core constitue une image séparée. Le chapitre Consolider vos serveurs avec Hyper V couvre en détail ce type d'installation.

Microsoft met à disposition plusieurs tableaux permettant de voir les différences entre les éditions serveurs :

Les différences sur les rôles sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/compare-roles.aspx

Pour une installation Core :

http://www.microsoft.com/windowsserver2008/en/us/compare-core-installation.aspx

Les différences sur les fonctionnalités sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/compare-features.aspx

Les différences sur le matériel sont disponibles à cette adresse :

http://www.microsoft.com/windowsserver2008/en/us/compare-specs.aspx

Pour les différences entre les éditions de Windows Vista :

http://www.microsoft.com/france/windows/products/windowsvista/editions/n/choose.mspx

© ENI Editions - All rigths reserved

Créer et déployer

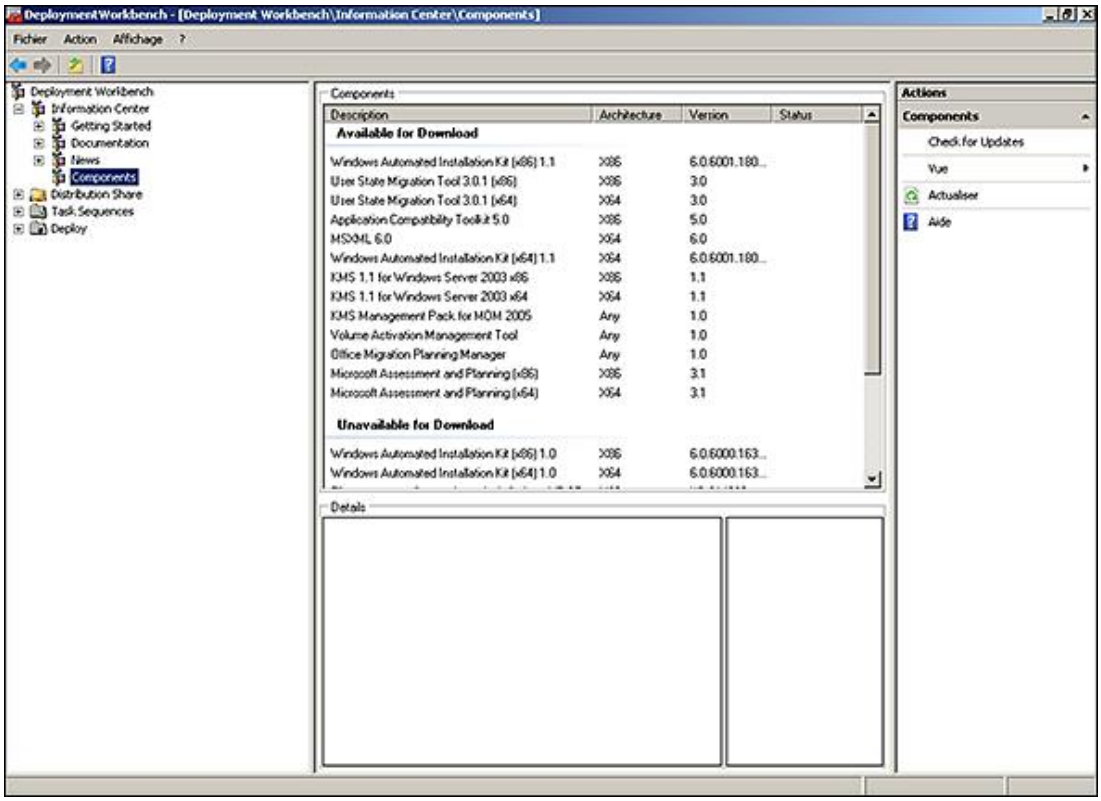
Cette section couvre la création et le déploiement des systèmes d'exploitation, à la fois clients et serveurs. Microsoft Deployment Toolkit est l'outil central, qui enrichit les outils natifs à travers une interface conviviale et un emplacement unique pour toutes les données nécessaires aux déploiements. Deux méthodes sont proposées : Lite Touch et Zero Touch.

MDT utilise plusieurs composants, dont WAIK (*Windows Automated Installation Kit*), Windows PE, et ImageX. Ces deux derniers sont fournis dans WAIK.

1. Microsoft Deployment Toolkit (MDT 2008)

Microsoft met gratuitement à votre disposition un outil afin d'accélérer votre projet de déploiement, MDT 2008. Il est disponible en téléchargement à cette adresse : http://www.microsoft.com/Downloads/ details.aspx?familyid=3BD8561F-77AC-4400-A0C1-FE871C461A89&displaylang=en

Une fois installé, l'interface de gestion se trouve dans **Démarrer - Tous les programmes - Microsoft Deployment Toolkit, Deployment Workbench**. Les composants complémentaires sont proposés en téléchargement depuis l'onglet **Components** dans la console :

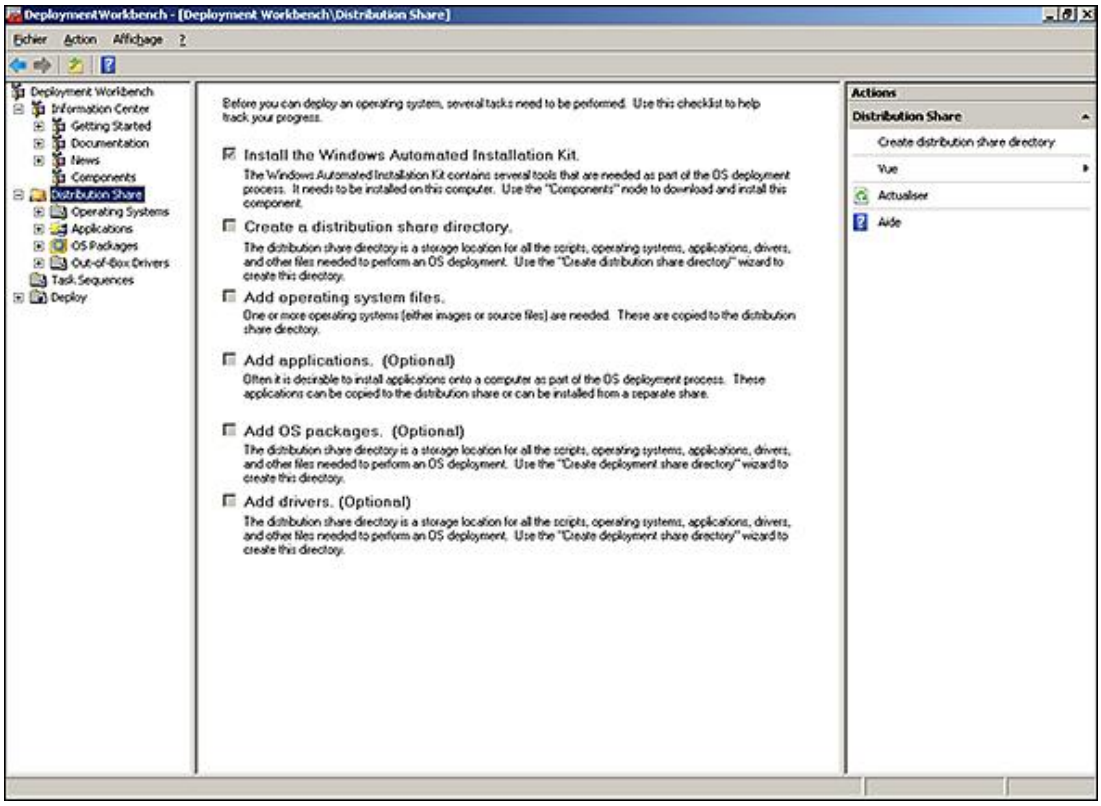

Deployment Workbench - [Deployment Workbench\Information Center\Components]
Fichier Action Affichage ?
Deployment Workbench
Information Center
Getting Started
Documentation
News
Components
Distribution Share
Task Sequences
Deploy
Components
Description Architecture Version Status
Available for Download
Windows Automated Installation Kit (x86) 1.1 X86 6.0.6001.180...
User State Migration Tool 3.0.1 (x86) X86 3.0
User State Migration Tool 3.0.1 (x64) X64 3.0
Application Compatibility Toolkit 5.0 X86 5.0
MSXML 6.0 X64 6.0
Windows Automated Installation Kit (x64) 1.1 X64 6.0.6001.180...
KMS 1.1 for Windows Server 2003 x86 X86 1.1
KMS 1.1 for Windows Server 2003 x64 X64 1.1
KMS Management Pack for MOM 2005 Any 1.0
Volume Activation Management Tool Any 1.0
Office Migration Planning Manager Any 1.0
Microsoft Assessment and Planning (x86) X86 3.1
Microsoft Assessment and Planning (x64) X64 3.1
Unavailable for Download
Windows Automated Installation Kit (x86) 1.0 X86 6.0.6000.163...
Windows Automated Installation Kit (x64) 1.0 X64 6.0.6000.163...
Details
Actions
Components
Check for Updates
Vue
Actualiser
Aide

Il faut au moins télécharger le composant **Windows Automated Installation Kit** (appelé aussi **WAIK**), en 32 ou 64 bits suivant votre environnement. MDT n'étant disponible qu'en anglais, il téléchargera ce composant en anglais. Pour télécharger la version française, il suffit de se rendre à cette page : http://www.microsoft.com/downloads/details.aspx? displaylang=fr&FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08

Tant que ce composant n'est pas présent, aucune des fonctions des nœuds **Distribution Share**, **Task Sequences** et **Deploy** ne fonctionnent. MDT pilote WAIK afin de vous assister dans sa mise en œuvre, et ne peut donc pas fonctionner sans celui-ci. En le téléchargeant, vous obtenez aussi Windows PE.

Une fois WAIK installé, l'arbre **Distribution Share** permet de visualiser l'état d'avancement des tâches à effectuer pour déployer des systèmes d'exploitation :

© ENI Editions - All rigths reserved


Deployment Workbench - [Deployment Workbench\Distribution Share]
Fichier Action Affichage ?
Deployment Workbench
Information Center
Getting Started
Documentation
News
Components
Distribution Share
Operating Systems
Applications
OS Packages
Out-of-Box Drivers
Task Sequences
Deploy
Before you can deploy an operating system, several tasks need to be performed. Use this checklist to help track your progress.
Install the Windows Automated Installation Kit.
The Windows Automated Installation Kit contains several tools that are needed as part of the OS deployment process. It needs to be installed on this computer. Use the "Components" node to download and install this component.
Create a distribution share directory.
The distribution share directory is a storage location for all the scripts, operating systems, applications, drivers, and other files needed to perform an OS deployment. Use the "Create distribution share directory" wizard to create this directory.
Add operating system files.
One or more operating systems (either images or source files) are needed. These are copied to the distribution share directory.
Add applications. (Optional)
Often it is desirable to install applications onto a computer as part of the OS deployment process. These applications can be copied to the distribution share or can be installed from a separate share.
Add OS packages. (Optional)
The distribution share directory is a storage location for all the scripts, operating systems, applications, drivers, and other files needed to perform an OS deployment. Use the "Create deployment share directory" wizard to create this directory.
Add drivers. (Optional)
The distribution share directory is a storage location for all the scripts, operating systems, applications, drivers, and other files needed to perform an OS deployment. Use the "Create deployment share directory" wizard to create this directory.
Actions
Distribution Share
Create distribution share directory
Vue
Actualiser
Aide

La prochaine étape est la création du partage contenant tout ce qui est nécessaire au déploiement. Pour cela, faites un clic droit sur le nœud **Distribution Share**, puis cliquez sur **Create distribution share directory**. Choisissez le dossier de destination et cliquez sur **Finish**. Les sous-dossiers suivants sont créés :

- **OEM** : tout ce qui est dans ce dossier sera copié sur la machine pendant le déploiement.
- **Applications** : contiendra les applications ajoutées dans le déploiement.
- **Captures** : contiendra les captures des systèmes d'exploitation.
- **Control** : contient les fichiers XML décrivant tout le contenu et configuration du partage.
- **Operating Systems** : contient les sources des systèmes d'exploitation.
- **Out-of-Box Drivers** : contiendra les pilotes supplémentaires nécessaires.
- **OS Packages** : contiendra les mises à jour Windows à intégrer.
- **Scripts** : contient des scripts VBS pour le déploiement Lite Touch et Zero Touch.
- **Tools** : contient des outils internes à MDT.

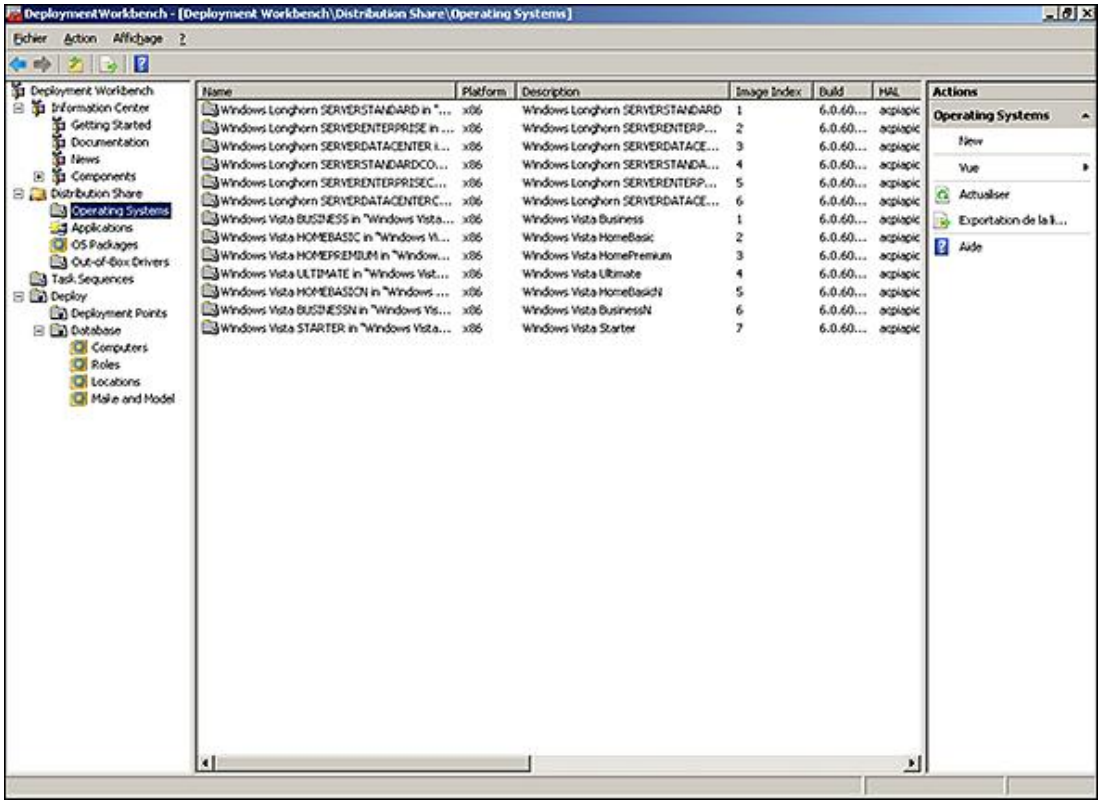
Les étapes suivantes sont :

- Ajouter des systèmes d'exploitation (depuis leur DVD…).
- Ajouter des applications (installation silencieuse…)
- Ajouter des mises à jour Windows.
- Ajouter des pilotes.
- Créer une séquence d'actions à effectuer.

© ENI Editions - All rigths reserved

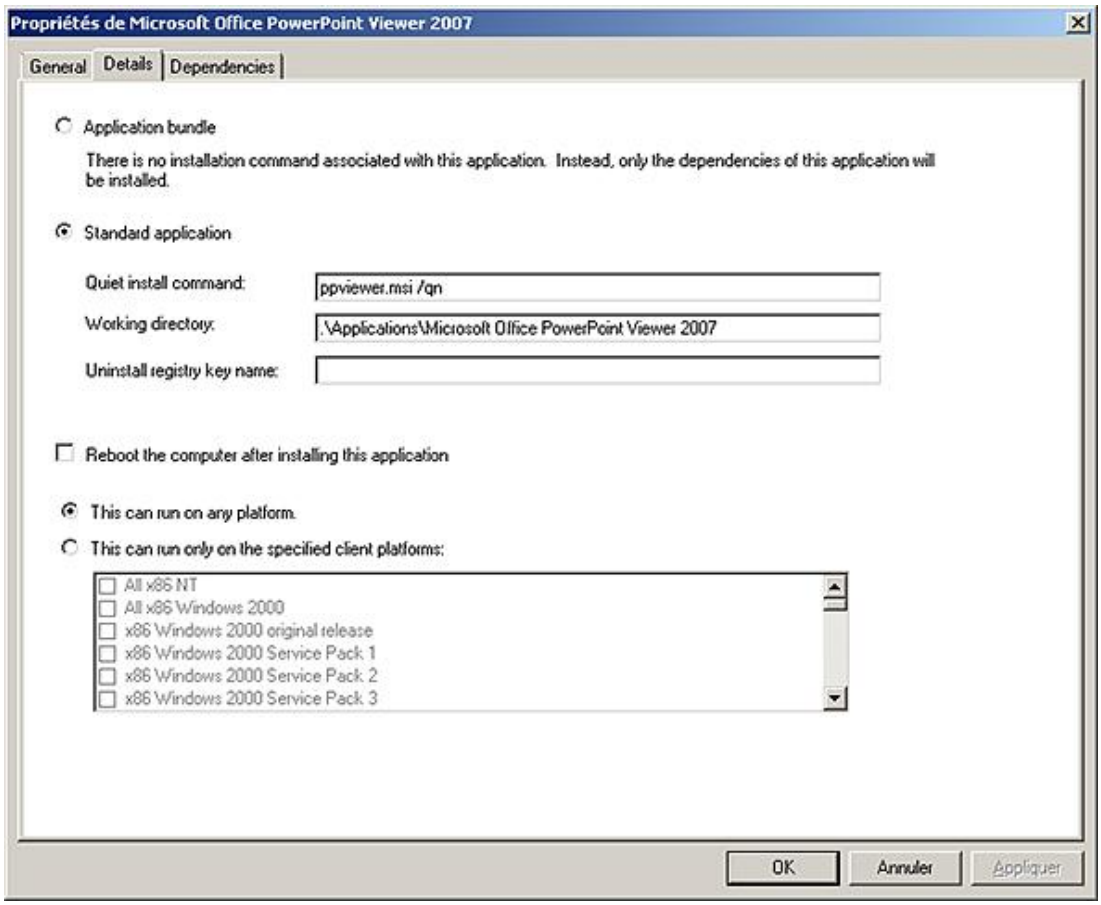
- Créer une base de données pour inventorier les machines déployées.

L'ajout de systèmes d'exploitation est très simple. Une fois les DVD ou autre importés, ils apparaissent comme ceci :

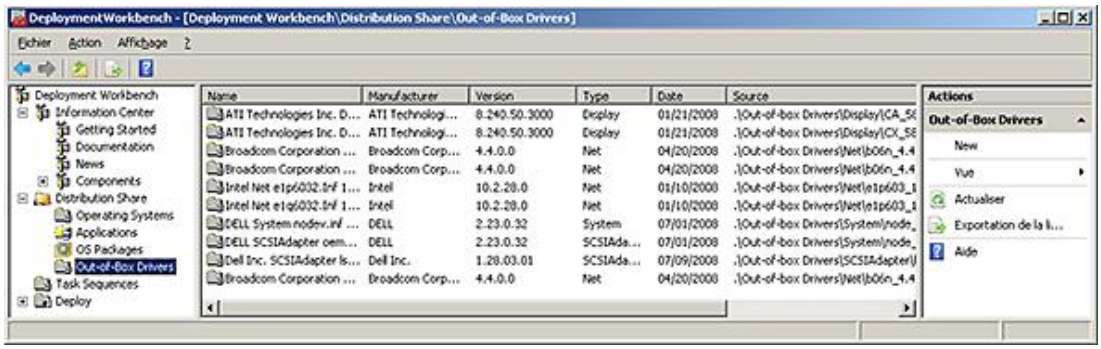

DeploymentWorkbench - [Deployment Workbench\Distribution Share\Operating Systems]
Fichier Action Affichage ?
Deployment Workbench
Information Center
Getting Started
Documentation
News
Components
Distribution Share
Operating Systems
Applications
OS Packages
Out-of-Box Drivers
Task Sequences
Deploy
Deployment Points
Database
Computers
Roles
Locations
Make and Model
Name Platform Description Image Index Build HAL
Windows Longhorn SERVERSTANDARD in "... x86 Windows Longhorn SERVERSTANDARD 1 6.0.60... acpiapic
Windows Longhorn SERVERENTERPRISE in ... x86 Windows Longhorn SERVERENTERP... 2 6.0.60... acpiapic
Windows Longhorn SERVERDATACENTER i... x86 Windows Longhorn SERVERDATACE... 3 6.0.60... acpiapic
Windows Longhorn SERVERSTANDARDCO... x86 Windows Longhorn SERVERSTANDA... 4 6.0.60... acpiapic
Windows Longhorn SERVERENTERPRISEC... x86 Windows Longhorn SERVERENTERP... 5 6.0.60... acpiapic
Windows Longhorn SERVERDATACENTERC... x86 Windows Longhorn SERVERDATACE... 6 6.0.60... acpiapic
Windows Vista BUSINESS in "Windows Vista... x86 Windows Vista Business 1 6.0.60... acpiapic
Windows Vista HOMEBASIC in "Windows Vi... x86 Windows Vista HomeBasic 2 6.0.60... acpiapic
Windows Vista HOMEPREMIUM in "Window... x86 Windows Vista HomePremium 3 6.0.60... acpiapic
Windows Vista ULTIMATE in "Windows Vist... x86 Windows Vista Ultimate 4 6.0.60... acpiapic
Windows Vista HOMEBASICN in "Windows ... x86 Windows Vista HomeBasicN 5 6.0.60... acpiapic
Windows Vista BUSINESSN in "Windows Vis... x86 Windows Vista BusinessN 6 6.0.60... acpiapic
Windows Vista STARTER in "Windows Vista... x86 Windows Vista Starter 7 6.0.60... acpiapic
Actions
Operating Systems
New
Vue
Actualiser
Exportation de la li...
Aide

L'ajout d'application à travers le nœud **Applications** permet d'installer des applications post déploiement. Il s'agit d'installations silencieuses, de fichiers MSI, etc. Vous pouvez ensuite les intégrer dans les séquences d'installations. Les propriétés suivantes sont disponibles :

© ENI Editions - All rigths reserved


Propriétés de Microsoft Office PowerPoint Viewer 2007
General
Details
Dependencies
Application bundle
There is no installation command associated with this application. Instead, only the dependencies of this application will be installed.
Standard application
Quiet install command:
ppviewer.msi /qn
Working directory:
.\Applications\Microsoft Office PowerPoint Viewer 2007
Uninstall registry key name:
Reboot the computer after installing this application
This can run on any platform.
This can run only on the specified client platforms:
All x86 NT
All x86 Windows 2000
x86 Windows 2000 original release
x86 Windows 2000 Service Pack 1
x86 Windows 2000 Service Pack 2
x86 Windows 2000 Service Pack 3
OK
Annuler
Appliquer

Le choix **Application bundle** permet de grouper des applications. L'ajout de mises à jour Windows se fait via le nœud **OS Packages**. C'est aussi simple que de fournir le dossier les contenants (fichiers .cab et .msu). Par défaut, elles appartiennent au groupe **All Packages**. Vous pouvez ajouter des groupes personnalisés afin de filtrer les mises à jour à appliquer dans les séquences d'installation. Le nœud **Out-of-Box-Drivers** contiendra tous vos pilotes. Il suffit de fournir le dossier les contenants (fichiers .inf). Au moment de l'importation, il est possible de spécifier des catégories, utilisables ensuite dans les séquences.



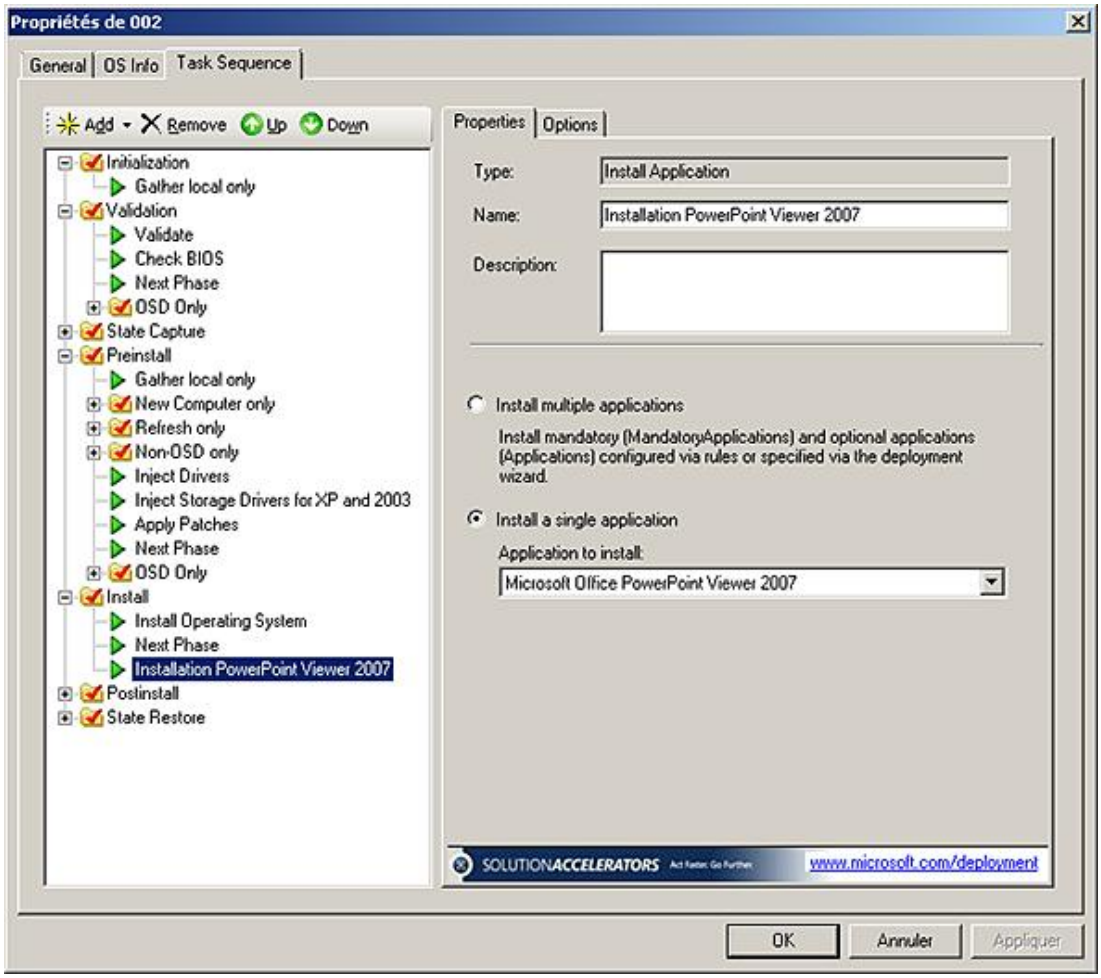
Le nœud **Task Sequences** est la clé de voute du logiciel. Il permet de rassembler toutes les briques précédentes afin d'en faire des scénarios d'installation. Lors de la création d'une séquence, seulement les options courantes sont proposées :

- Un identifiant unique, titre, description.
- Un masque de séquence.
- Un système d'exploitation parmi la liste du nœud **Operating Systems**.
- Indiquer ou non un numéro de série (période d'essai le cas échéant).
- Le nom, la page par défaut d'Internet Explorer.

© ENI Editions - All rigths reserved

- Le mot de passe Administrateur local (ou le demander au premier lancement).

Une fois créée, il faut ouvrir les propriétés de la séquence, dans l'onglet **Task Sequence**, pour découvrir toutes les capacités des séquences :



Les ajouts possibles sont regroupés par thèmes :

- Général
    - Exécuter une ligne de commande.
    - Positionner une variable.
    - Exécuter une commande en tant que.
    - Redémarrer.
    - Collecter des informations.
    - Installer des mises à jour au premier lancement.
    - Valider.
    - Installer une ou des applications présentes dans le nœud **Applications**.
- Disques
    - Partitionner et formater un disque.

© ENI Editions - All rigths reserved

        - Activer BitLocker.
    - Images
        - Installer un système d'exploitation.
    - Paramètres
        - Appliquer un paramétrage réseau (IP, DNS, WINS).
        - Capturer le paramétrage réseau existant.
    - Rôles
        - Installer et configurer des rôles et fonctionnalités.
        - Configurer le serveur DHCP, DNS, Active Directory, et enfin autoriser le DHCP.

Les scénarios possibles sont très larges lors du déploiement :

- Sauvegarde ou non des profils utilisateurs locaux sur un partage réseau (avec restauration).
- Capture des paramètres réseaux avant la réinstallation, puis restauration de ceux-ci.
- Installation et configuration des rôles communs Windows Server 2008.
- Gestion de BitLocker avec paramétrage :
    - Moyen de stockage (TPM, USB, les deux).
    - Création d'une clé de recouvrement dans l'Active Directory.
    - Attendre la fin de l'encryption avant de continuer.
- Injections de pilotes et mises à jour Windows.

Il reste ensuite à définir un point de déploiement, dans le nœud **Deploy - Deployment Points**. Les possibilités sont :

- le partage local à la machine où s'éxecute MDT 2008 ;
- un partage local ou distant ne contenant qu'un jeu de la configuration ;
- un média de stockage amovible (DVD, USB) ;
- une intégration à SMS 2003.

Les séquences sont stockées dans le sous-dossier **Control du partage** créé précédemment, avec l'arborescence suivante :

- {GUID}
    - **Bootstrap.ini** : fichier de configuration quand la machine à déployer ne peut pas se connecter au point de déploiement.
    - **CustomSettings.ini** : fichier de configuration commun à toutes les séquences.

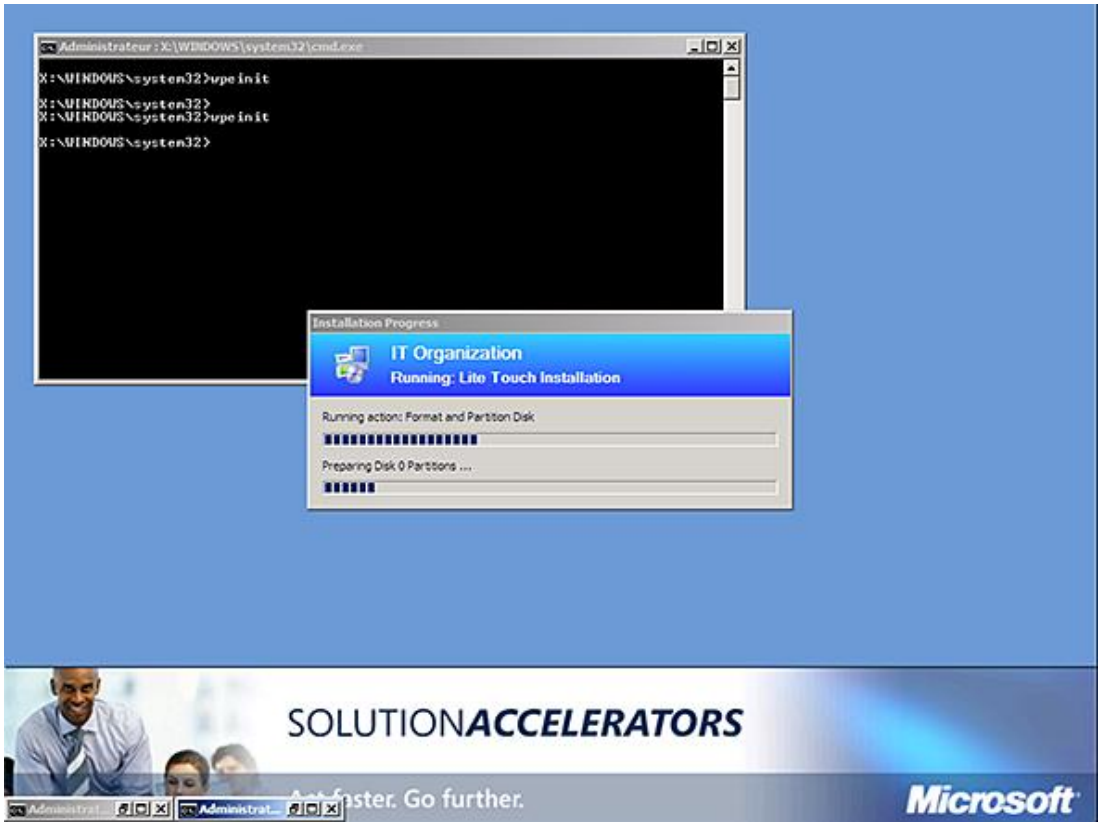
© ENI Editions - All rigths reserved

- {Numéro de séquence}
    - **TS.xml** : contient des métadonnées sur la séquence.
    - **Unattend.xml** : contient les valeurs pour le sysprep.

Le déploiement via un média amovible est la plus basique, mais très efficace quand la connectivité réseau est limitée. Dans le dossier de destination, vous trouverez une image ISO bootable, LiteTouchPE_x86.iso ou LiteTouchPE_x64.iso suivant votre environnement.

Window PE est l'environnement de préinstallation de Windows. Il s'agit d'un Windows très léger, permettant d'exécuter un ensemble d'outils pour déployer un système d'exécution Windows. L'image WIM générée par MDT utilise Windows PE. Dans ce type d'environnement, le moteur vbscript est notamment disponible. Les écrans graphiques MDT sont des vbscript et HTA (*HTML Applications*). Windows PE ayant ses fichiers en mémoire, il est possible de partitionner et formater tout le stockage disponible, notamment la partition système. Certains outils, comme USMT et ImageX, fonctionnent dans ce type d'environnement, ce qui permet de sauvegarder les données de la machine avant sa réinstallation par exemple. La version actuelle est la 2.1, qui correspond à Windows Vista Service Pack1 et Windows Server 2008.

Voici par exemple l'environnement fourni par MDT :



Pour information, la version MDT 2010 est en Beta, afin d'intégrer Windows 7 et Windows 2008 R2.

2. Lite Touch

La solution Lite Touch permet d'industrialiser votre déploiement sans pour autant avoir l'infrastructure de gestion Microsoft, System Center Configuration Manager 2007. La solution reste simple à mettre en œuvre tout en étant très efficace, car il utilise le moteur de séquence de ce dernier, en version autonome. Le déploiement doit être initié manuellement, mais vous êtes guidé à travers des écrans graphiques pour effectuer celui-ci.

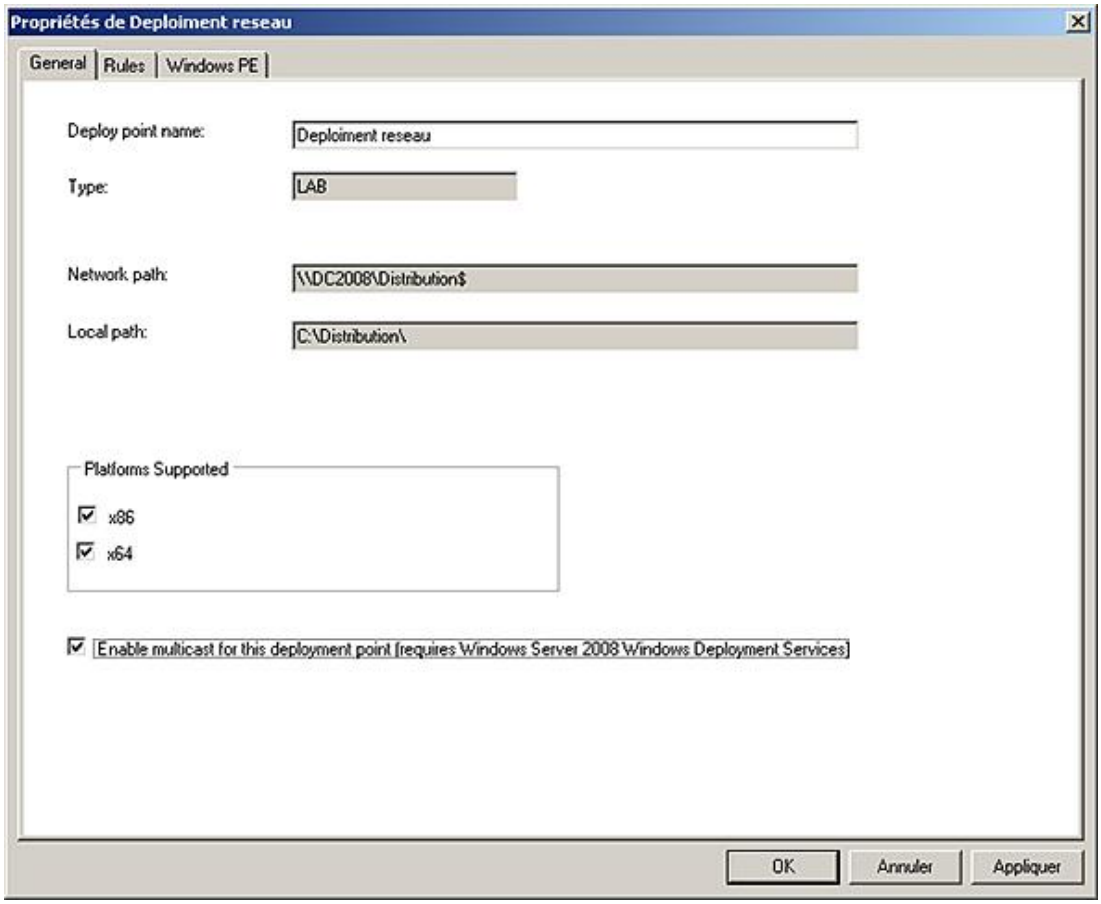
Au-delà d'une image ISO comme vu précédemment, le déploiement via le réseau est possible en utilisant WDS (dont l'installation est couverte plus loin). Il suffit de créer un point de déploiement de type partage depuis MDT. Une fois terminé, vous y trouverez un sous-dossier **boot**, contenant deux images de démarrage WIM (x64 et x86). Vous devez ensuite spécifier dans **CustomSettings.ini** la variable `DeployRoot=\\%WDSServer%\Distribution$`, sous la section [Default].

Il faut remplacer `Distribution$` par le nom de votre partage si vous n'avez pas laissé le nom par défaut. Il faut ensuite mettre à jour le point de distribution, en effectuant un clic droit dessus, puis choisir **Update**. Il suffit ensuite :

© ENI Editions - All rigths reserved

- d'importer ces deux images WIM dans WDS ;
- de démarrer une machine via PXE.

L'utilisation du multicast pour le déploiement est même disponible :



Avant de déployer une image, certaines questions seront posées via des interfaces graphiques. Il est possible d'augmenter l'automatisation en les évitant. Vous devrez fournir les réponses à ces questions dans le fichier **CustomSettings.ini**. Voici les étapes pouvant être évitées si les variables suivantes sont positionnées à **YES** (en majusucule) dans le fichier **CustomSettings.ini**, section [Default]. À chaque écran correspond une variable pour l'éviter, ainsi qu'une ou plusieurs variables afin de renseigner les informations demandées par cet écran :

`SkipAdminPassword` : ne demande pas de mot de passe administrateur local.

- Automatiser par `AdminPassword`=monmotdepasseadmin. Le mot de passe sera stocké en clair dans le fichier, vous devez donc changer ce mot de passe ultérieurement. Il est même conseillé de le changer régulièrement de façon automatisée sur l'ensemble de vos machines.

`SkipApplications` : ne propose pas d'installer des applications.

- Automatiser par `Applications001={GUID de l'application trouvée dans control\Applications.xml}`

`SkipAppsOnUpgrade` : ne propose pas d'installer des applications si c'est une mise à jour.

`SkipBDDWelcome` : évite la fenêtre d'accueil.

`SkipBitLocker` : ne propose pas BitLocker.

`SkipBitLockerDetails` : ne demande pas la configuration de BitLocker.

`SkipTaskSequence` : ne propose pas le choix de la séquence.

- Automatiser par `TaskSequenceID={Identifiant de séquence}`

© ENI Editions - All rigths reserved

`SkipCapture` : ne propose pas l'utilisation de capture.

- Automatiser par `DoCapture=NO|YES|PREPARE`

`SkipComputerBackup` : ne propose pas la sauvegarde de l'ordinateur.

- Automatiser par `ComputerBackupLocation=NETWORK|AUTO|NONE`
    - `NETWORK` fait une sauvegarde sur le réseau.
    - `AUTO` fait une sauvegarde locale s'il y a suffisamment d'espace disque, sinon sur le réseau.
    - `NONE` ne fait aucune sauvegarde.

Si vous souhaitez faire une sauvegarde sur le réseau, il faut aussi utiliser ces deux variables :

```
BackupShare=\\DC2008\Backup$
```

```
BackupDir=%ComputerName%
```

Pour que la sauvegarde fonctionne, les permissions doivent être les suivantes sur le partage utilisé :

- Objet ordinateurs et utilisateurs du domaine en création de dossiers et ajouts de données.
- Créateur propriétaire en contrôle total.

`SkipComputerName` : ne demande pas le nom de l'ordinateur.

- Automatiser par `ComputerName=%SerialNumber%` par exemple.

`SkipDeploymentType` : ne demande pas le type de déploiement.

- Automatiser par `DeploymentType=NEWCOMPUTER`. Il peut prendre les valeurs NEWCOMPUTER, REFRESH, REPLACE, UPGRADE

`SkipDomainMembership` : ne propose pas de joindre un domaine.

- Automatiser par `JoinDomain=MASOCIETE`. Les variables additionnelles sont :

```
MachineObjectOU=OU=Mes_Serveurs,DC=masociete,DC=local
```

```
DomainAdmin=Administrateur
```

```
DomainAdminDomain=MASOCIETE
```

```
DomainAdminPassword=motdepassecomplexe
```

Le mot de passe étant stocké en clair, vous devriez utiliser un compte qui n'a que le droit de joindre les machines au domaine.

`SkipFinalSummary` : ne montre pas la fenêtre de résumé finale de la séquence.

`SkipLocaleSelection` : ne propose pas de choisir les paramètres régionaux.

- Automatiser par :

```
UserLocaleAndLang="fr-FR,fr-FR"
```

```
KeyboardLocale="040c :0000040c"
```

© ENI Editions - All rigths reserved

UserLocale=fr-FR et UILanguage=fr-FR

SkipPackageDisplay : ne propose pas de package complémentaire.

SkipProductKey : ne demande de numéro de série.

SkipSummary : ne montre pas le résumé.

SkipTimeZone : ne demande pas le fuseau horaire.

- Automatiser par TimeZone=''110'' et TimeZoneName=''W. Europe Standard Time''.

SkipUserData : ne demande pas s'il faut sauvegarder les profils utilisateurs.

- Automatiser par UserDataLocation=NETWORK|AUTO|NONE.
    - NETWORK fait une sauvegarde sur le réseau.
    - AUTO fait une sauvegarde locale si il y a suffisamment d'espace, sinon sur le réseau.
    - NONE ne fait aucune sauvegarde.

Si vous souhaitez faire une sauvegarde sur le réseau, il faut aussi utiliser ces deux variables :

```
UDShare=\\DC2008\Profiles$
```

```
UDDir=%ComputerName%
```

Et enfin, pour renseigner le compte à utiliser pour accéder au partage contenant les ressources MDT :

```
USERID=Administrateur
UserPassword=motdepassecomplexe
UserDomain=MASOCIETE
```

Votre fichier **CustomSettings.ini** pourrait donc ressembler à ceci :

```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
OSInstall=Y
SkipBDDWelcome= YES
SkipCapture=YES
SkipAppsOnUpgrade=YES
SkipFinalSummary=YES
SkipPackageDisplay= YES
SkipProductKey=YES
SkipSummary=YESUSERID=Administrateur
UserPassword= motdepassecomplexe
UserDomain=MASOCIETE

SkipComputerBackup=YES
ComputerBackupLocation= NONE

SkipAdminPassword=YES
AdminPassword=monmotdepasseadminlocal

SkipApplications=YES
Applications001={73823faf-bb78-4491-a053-b47afb5553c4}

SkipTaskSequence=YES
TaskSequenceID= 001

SkipComputerName=YES
ComputerName=%SerialNumber%
```


© ENI Editions - All rigths reserved

```
SkipDeploymentType=YES
DeploymentType=NEWCOMPUTER

SkipDomainMembership=YES
JoinDomain=MASOCIETE
MachineObjectOU=OU=Mes_Serveurs,DC=masociete,DC=local
DomainAdmin= Administrateur
DomainAdminDomain=MASOCIETE
DomainAdminPassword= motdepassecomplexe

SkipLocaleSelection=YES
UserLocaleAndLang="fr-FR,fr-FR"
KeyboardLocale= "040c :0000040c
"UserLocale=fr-FR
UILanguage=fr-FR

SkipTimeZone=YES
TimeZone="110"
TimeZoneName="W. Europe Standard Time"

SkipUserData=YES
UserDataLocation=NONE
DeployRoot=\\DC2008\Distribution$
```

L'intégration avec WSUS est prévue dans MDT. Si le système d'exploitation à déployer est antérieur à Windows Server 2008 ou Windows Vista, le client Windows Update doit être mis à jour. Il est téléchargeable ici :

Version x86 : http://go.microsoft.com/fwlink/?LinkID=100334

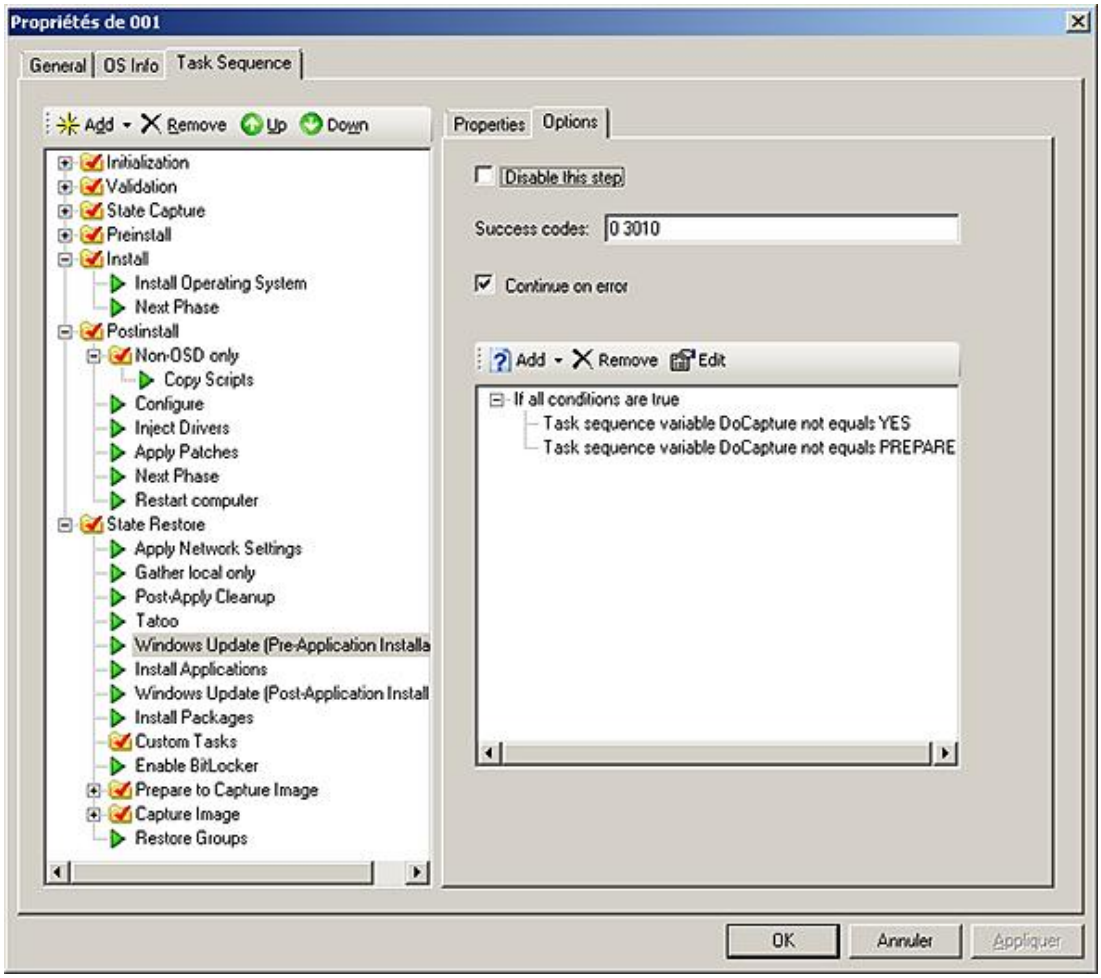
Version x64 : http://go.microsoft.com/fwlink/?LinkID=100335

MDT peut les déployer automatiquement si ces exécutables sont copiés dans le sous-dossier Tools\x86 et Tools\x64 respectivement. Si vous déployez Windows XP Service Pack 2 ou 3, ou Windows Server 2003 Service Pack 2, une alerte de sécurité bloquera cette installation car il est installé depuis le partage réseau. Pour contourner ce problème, il faudra alors installer l'agent comme une application standard depuis MDT avec comme commande `WindowsUpdateAgent30-[platforme].exe /quiet /norestart /wuforce`.

Par défaut, la machine essaiera de se connecter aux serveurs Microsoft Windows Update sur Internet. Si vous avez un serveur WSUS, vous pouvez l'indiquer à MDT en ajoutant la variable `WSUSServer=http://monserveur` dans le fichier **CustomSettings.ini.** Si vous spécifiez un serveur WSUS mais que le client n'est pas à jour, MDT essaiera de le télécharger depuis Internet.

Il ne reste plus qu'à activer les deux étapes Windows Update dans la séquence (Pre et Post), car elles sont désactivées par défaut :

© ENI Editions - All rigths reserved



Une autre approche est de déployer complètement une machine, la configurer entièrement, en installant les applications et mises à jour par exemple, puis de la capturer à travers Lite Touch. Cela deviendra votre image de référence, qu'il vous suffira de déployer, en faisant un sysprep. Sysprep permet de rendre unique une machine, en ce qui concerne son nom et son SID (*Security IDentifier*). C'est pour cette raison que vous ne pouvez pas joindre un domaine AD pendant une phase de capture. La phase de sysprep est automatiquement incluse par MDT (phase *Copy sysprep files*). Un point d'attention, lors d'une capture effectuée par Lite Touch, reste l'utilisation d'antivirus, qui peut poser des problèmes.

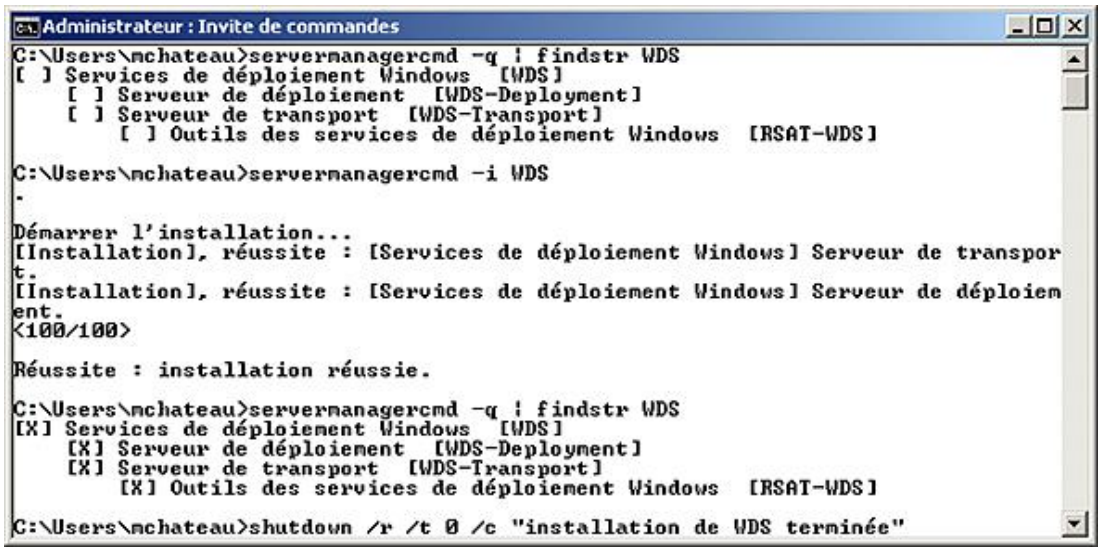
La migration des profils utilisateur est faite via le composant USMT (*User State Migration Tool*). Il n'est pas nécessaire de l'installer sur le serveur de déploiement. Tout comme pour le client Windows Update, il faut télécharger les installeurs 32 et 64 bits et les copier dans les sous-dossiers Tools\x86 et Tools\x64. Ils sont disponibles en téléchargement ici : http://www.microsoft.com/downloads/details.aspx?FamilyID= 799ab28c-691b-4b36-b7ad-6c604be4c595&displaylang=en#filelist

MDT offre la possibilité d'inventorier toutes les machines déployées dans une base de données SQL Server. Si vous le souhaitez, vous pouvez utiliser une base SQL Express. Cette version de SQL Server est gratuite, et suffit à ce besoin. Elle est téléchargeable chez Microsoft : http://www.microsoft.com/ downloads/details.aspx?displaylang=fr&FamilyID= 7522a683-4cb2-454e-b908-e805e9bd4e28

3. WDS

L'installation du rôle WDS est très simple, mais nécessite un redémarrage du serveur. Les pré-requis sont un domaine Active Directory, le service DNS et DHCP sur le réseau, ainsi qu'une partition NTFS pour le stockage. Afin d'installer le rôle, depuis une ligne de commande, exécutez la commande `servermanagercmd -i WDS` :

© ENI Editions - All rigths reserved


Administrateur : Invite de commandes
C:\Users\mchateau>servermanagercmd -q | findstr WDS
[ ] Services de déploiement Windows [WDS]
[ ] Serveur de déploiement [WDS-Deployment]
[ ] Serveur de transport [WDS-Transport]
[ ] Outils des services de déploiement Windows [RSAT-WDS]
C:\Users\mchateau>servermanagercmd -i WDS
.
Démarrer l'installation...
[Installation], réussite : [Services de déploiement Windows] Serveur de transport.
[Installation], réussite : [Services de déploiement Windows] Serveur de déploiement.
<100/100>
Réussite : installation réussie.
C:\Users\mchateau>servermanagercmd -q | findstr WDS
[X] Services de déploiement Windows [WDS]
[X] Serveur de déploiement [WDS-Deployment]
[X] Serveur de transport [WDS-Transport]
[X] Outils des services de déploiement Windows [RSAT-WDS]
C:\Users\mchateau>shutdown /r /t 0 /c "installation de WDS terminée"

Trois composants ont été installés :

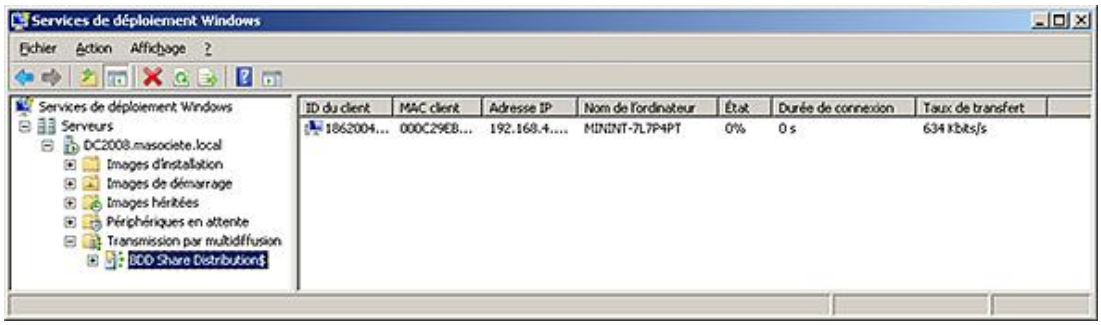
- **Serveur de déploiement** : il s'agit du composant principal.
- **Serveur de transport** : ce composant peut être installé tout seul en environnement restreint (sans Active Directory, DHCP, DNS…). Il est aussi utilisé par le composant principal.
- **Outils des services de déploiement Windows** : composants d'administrations.

Une fois installé, l'interface de gestion se trouve dans **Démarrer - Outils d'administration - Services de déploiement Windows**. Étendez les nœuds jusqu'au nom de votre serveur et sélectionnez **Configurer le serveur**. Choisissez ensuite un dossier pour le stockage des images (**%systemdrive%\RemoteInstall** par défaut). La volumétrie de ce dossier pouvant être importante, une alerte est émise si la partition système est utilisée. Si nécessaire, il est possible de réduire à chaud les volumes depuis le gestionnaire de disques, afin de disposer d'un lecteur dédié à ce stockage.

WDS peut être restreint afin de répondre uniquement aux clients connus. Pour qu'un client soit connu, il faut qu'il ait déjà joint l'Active Directory antérieurement, ou qu'un objet ordinateur ait été créé manuellement dans Active Directory avec le bon identifiant. L'identifiant utilisé est affiché au démarrage de la machine cliente, au moment de la recherche de PXE (GUID). Un mode d'approbation est aussi possible, l'administrateur visualisant les demandes de clients inconnus en attentes.

Pour un déploiement massif, le mode multicast est très adapté. Il permet de ne pas inonder le réseau en envoyant tous les octets individuellement à chaque machine. À la place, les machines s'inscrivent à l'adresse multicast, WDS n'envoyant alors qu'une fois les données à cette adresse pour toutes les machines. S'agissant de multicast IGMP, il faut que vos équipements réseaux le supportent. Si ce n'est pas le cas, le switch les traitera comme des diffusions, et inondera donc alors tout le réseau.

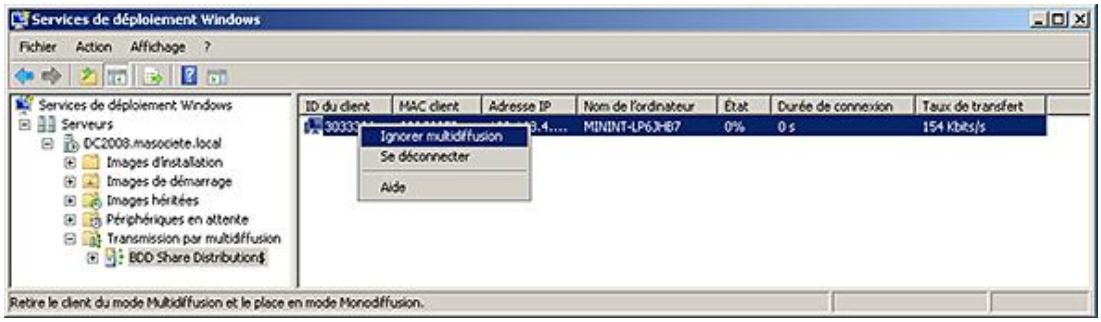
Si des machines arrivent pendant le déploiement, elles récupèrent les données envoyés jusqu'à la fin, puis WDS enverra les données manquantes à ces machines, qui sont donc capables de recevoir les données dans le désordre. Outre le gain réseau, le serveur est capable de déployer plus de machine à la fois car il ne lit qu'une fois les données à déployer. Cela réduit donc très fortement les accès au stockage disque. La liste des machines en cours de déploiement, ainsi que leur débit réseau est affichée depuis la console WDS :



La vitesse de déploiement de l'ensemble des machines est égale à la vitesse de déploiement de la machine la plus lente. S'il n'y a, par exemple, que des machines rapides sauf une, celle-ci empêchera les autres de se déployer plus vite. Le serveur n'émettant les paquets réseaux qu'une fois, il doit attendre qu'elles soient toutes prêtes à recevoir le prochain paquet. Dans la fenêtre ci-dessus, la colonne **Taux de transfert** permet de déterminer la vitesse de chaque machine pendant le déploiement. Si une machine est clairement plus lente que les autres, vous pouvez changer son

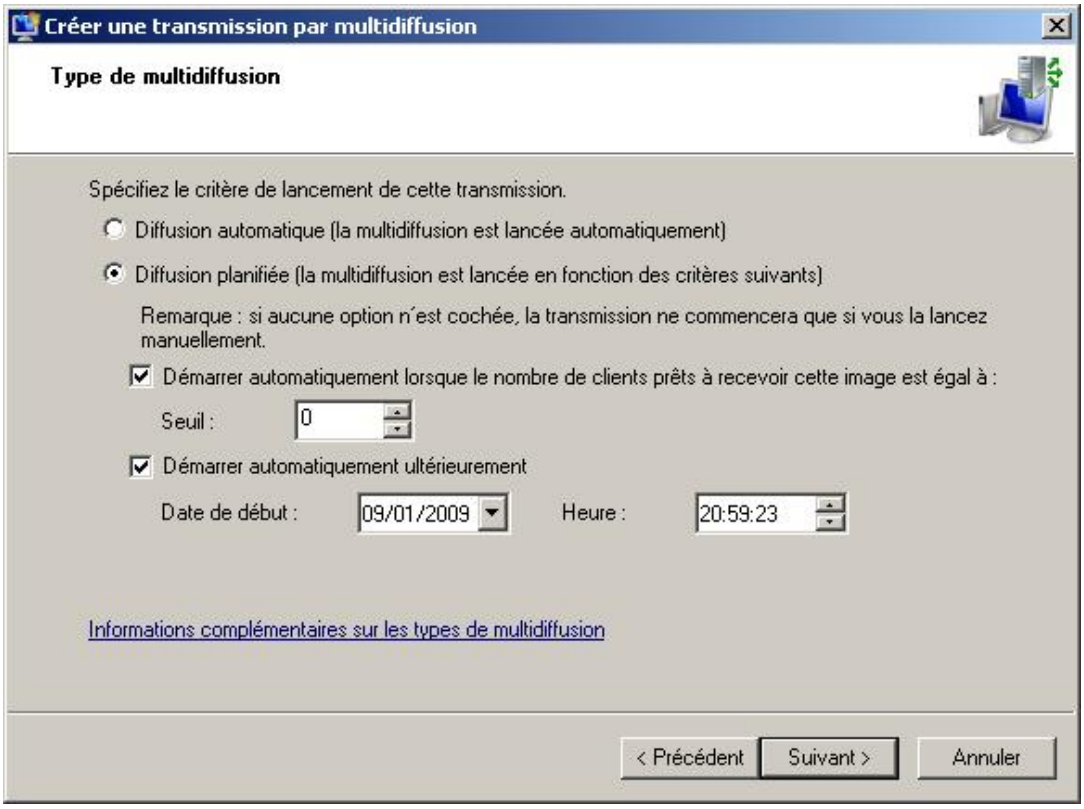
© ENI Editions - All rigths reserved

mode de déploiement en partage de fichier, afin qu'elle ne ralentisse plus les autres. Il suffit pour cela de faire un clic droit sur la machine et de choisir **Ignorer multidiffusion** :



La transmission par multidiffusion, créée par défaut par MDT 2008, est de type automatique. C'est-à-dire que le déploiement commence dès qu'un client demande une multidiffusion. WDS propose cependant aussi une multidiffusion planifiée. Cette planification peut se faire sur deux critères :

- le nombre de clients en attente de déploiement ;
- une date et une heure où déclencher le déploiement.


Créer une transmission par multidiffusion
Type de multidiffusion
Spécifiez le critère de lancement de cette transmission.
Diffusion automatique (la multidiffusion est lancée automatiquement)
Diffusion planifiée (la multidiffusion est lancée en fonction des critères suivants)
Remarque : si aucune option n'est cochée, la transmission ne commencera que si vous la lancez manuellement.
Démarrer automatiquement lorsque le nombre de clients prêts à recevoir cette image est égal à :
Seuil :
0
Démarrer automatiquement ultérieurement
Date de début :
09/01/2009
Heure :
20:59:23
Informations complémentaires sur les types de multidiffusion
< Précédent
Suivant >
Annuler

Les deux critères peuvent être utilisés en même temps. Si aucun des deux n'est sélectionné, il faudra démarrer manuellement la multidiffusion. Même s'il s'agit d'un déploiement planifié, un démarrage manuel est toujours possible par ailleurs.

© ENI Editions - All rigths reserved

Aller plus loin

Le déploiement de vos serveurs constitue le premier socle technique. Il reste maintenant à automatiser l'installation de vos applications, ce qui peut s'avérer long et difficile. La virtualisation crée un nouveau besoin : le déploiement à la demande d'environnement. Il n'est plus question de faire du paramétrage manuel dans ce contexte.

1. Microsoft Application Compatibility Toolkit

Cet outil vous aide à résoudre les incompatibilités applicatives avec Windows Vista. Les incompatibilités portent généralement sur :

- l'élévation de privilège (UAC) ;
- les tentatives d'écritures dans %ProgramFiles%.

Pour le télécharger gratuitement, il suffit de se rendre ici : http://www.microsoft.com/downloads/details.aspx?FamilyId=24DA89E9-B581-47B0-B45E-492DD6DA2971&displaylang=en

Si vous ne pouvez pas modifier l'application, il vous est possible d'implémenter des *shims*, afin de modifier à la volée les appels posant problèmes pendant l'exécution. Le mot shim désigne une librairie qui convertit l'appel d'une API en un autre. Le programme **Compatibility Administrator** permet de visualiser les shims utilisés par Microsoft pour rendre compatible 5649 applications. Pour y parvenir, 340 shims sont disponibles.

En ajoutant l'argument **-x** au programme ci-dessus, 772 shims sont disponibles. Ils sont masqués par défaut car rarement nécessaires. Il est ainsi possible de « faire croire » à votre application que le système d'exploitation est Windows XP, ou qu'Internet Explorer 6 est présent. Les développeurs ont tendance à faire ces vérifications bloquantes pour être certains qu'il n'y ait pas de problème, alors que la plupart du temps, il n'y a pas d'incompatibilité avérée. Une fois l'application rendue compatible avec Windows Vista ou Windows Server 2008, il faudra installer la base de données sur les machines l'utilisant.

Afin de faciliter le diagnostic, le programme **Standard User Analyzer Wizard** guide étape par étape :

- la préparation avant l'exécution.
- l'éxécution de l'application, en réalisant toutes les actions posant problèmes.
- l'analyse et la proposition de shims.

2. Environnement à la demande

Le déploiement de machines virtuelles peut devenir très consommateur, surtout s'il s'agit d'environnements à la demande pour du développement. System Center Virtual Machine Manager 2007 offre notamment un portail d'environnement à la demande.

Vous pouvez créer une séquence pour vos environnements virtuels afin d'installer automatiquement les outils additionnels. Hyper-V étant compatible avec le démarrage PXE, vous pouvez installer vos machines virtuelles directement via le réseau avec WDS. Vous n'avez ainsi qu'un point central qui contient toutes vos images et applications pendant le déploiement, au lieu d'avoir une image à part pour la génération de machines virtuelles.

3. ImageX

ImageX est un outil en ligne de commande permettant de gérer et modifier les images WIM. Le format WIM a notamment une propriété intéressante, il est basé sur les fichiers et non les clusters, comme pour les formats ISO. Cela permet notamment de ne stocker dans l'image qu'un seul exemplaire de chaque fichier, même s'il est présent plusieurs fois d'un point de vue logique (*Single Instance Storage*).

L'outil accepte les arguments suivants :

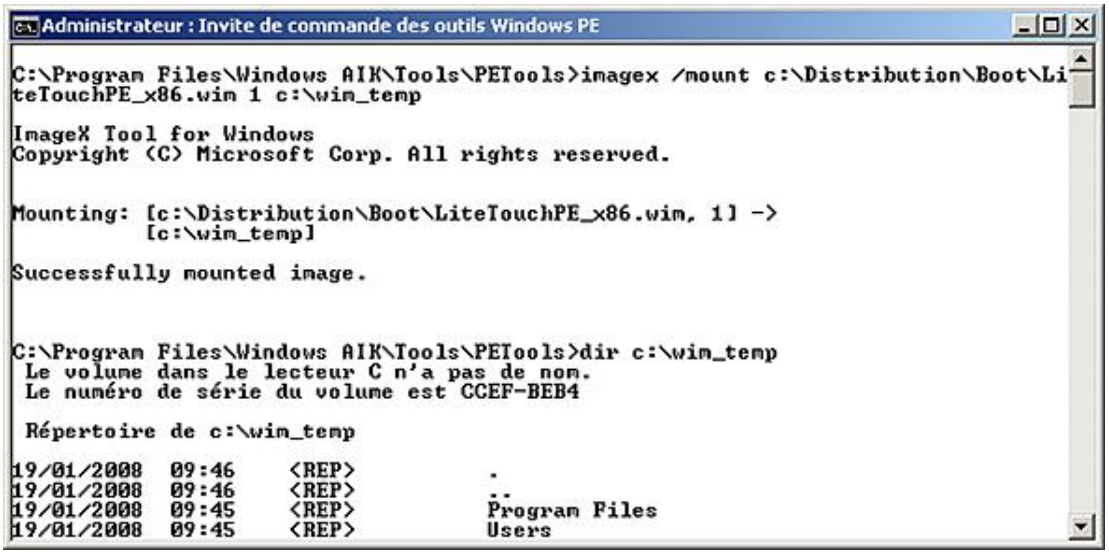
- **APPEND** : combine deux images ensembles.
- **APPLY** : applique une image à un dossier.

© ENI Editions - All rigths reserved

- **CAPTURE** : capture une partition dans une image wim.
- **DELETE** : efface un volume au sein d'un fichier wim.
- **DIR** : liste les fichiers contenus dans un fichier wim.
- **EXPORT** : copie un volume d'un fichier wim dans un autre fichier wim.
- **INFO** : affiche la description XML d'un fichier wim.
- **SPLIT** : sépare un fichier wim en deux fichiers wim.
- **MOUNT** : monte en lecture seule un fichier wim dans un répertoire.
- **MOUNTRW** : monte en lecture et écriture un fichier wim dans un répertoire.
- **UNMOUNT** : démonte un fichier wim d'un répertoire.

Cet outil est utile si vous souhaitez modifier l'image générée par MDT.

Par exemple, pour monter l'image WIM LiteTouch dans un dossier, il faut exécuter : `imagex /mount c:\Distribution\Boot\LiteTouchPE_x86.wim 1 c:\wim_temp`.


Administrateur : Invite de commande des outils Windows PE
C:\Program Files\Windows AIK\Tools\PETools>imagex /mount c:\Distribution\Boot\LiteTouchPE_x86.wim 1 c:\wim_temp
ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Mounting: [c:\Distribution\Boot\LiteTouchPE_x86.wim, 1] ->
[c:\wim_temp]
Successfully mounted image.
C:\Program Files\Windows AIK\Tools\PETools>dir c:\wim_temp
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est CCEF-BEB4
Répertoire de c:\wim_temp
19/01/2008 09:46 <REP> .
19/01/2008 09:46 <REP> ..
19/01/2008 09:45 <REP> Program Files
19/01/2008 09:45 <REP> Users

L'exécutable ImageX se trouve à différents endroits :

- dans le sous-dossier **Tools\PeTools** du répertoire d'installation de Windows AIK ;
- dans **X:\Deploy\Tools\x86 ou X:\Deploy\Tools\x64** depuis l'environnement de démarrage Windows PE construit par MDT.

4. Zero touch avec SCCM 2007

Utiliser System Center Configuration Manager 2007 permet d'automatiser entièrement le déploiement des machines. Depuis la console SCCM, vous pouvez directement programmer et effectuer des déploiements sur des machines existantes, sans devoir vous déplacer devant la machine pour démarrer en PXE et choisir la séquence.

Vous êtes maintenant prêt à déployer vos serveurs et postes de travail. D'un point de vue technique, cela n'a jamais été aussi simple et souple, notamment avec MDT 2008. Continuer à faire les installations à la main serait vraiment une perte de temps et de qualité !

© ENI Editions - All rigths reserved

Introduction

Ce chapitre sera consacré au rôle Terminal Services dans Windows Server 2008. Vous pratiquez certainement un usage intensif de ce service pour administrer votre parc de serveurs au quotidien. Après avoir couvert cet usage simple mais néanmoins critique, la puissance du rôle TSE sera mise au jour. Cela couvre notamment la publication d'applications et non plus juste d'un bureau, ainsi que l'accès à ces applications à travers une passerelle Web.

© ENI Editions - All rigths reserved

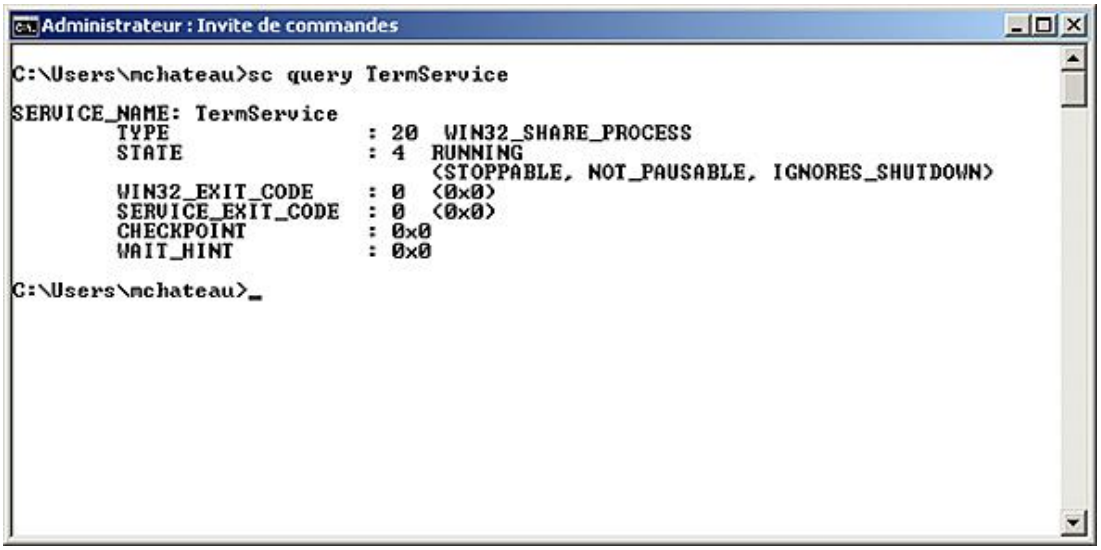
Mise en œuvre de Terminal Services

D'un point de vue technique, le service Windows Terminal est déjà installé par défaut avec Windows 2008 Server. Contrairement aux versions précédentes de Windows, il tourne désormais avec le compte « Service Réseau » au lieu du compte système local. La sécurité du système est améliorée, car une faille dans le service a moins d'impact qu'auparavant. Comme expliqué dans la base de connaissance Microsoft (KB946399), le compte « Service Réseau » a besoin de trois privilèges pour lancer le service TSE :

- Ajuster les quotas de mémoire pour un processus (SeIncreaseQuotaPrivilege).
- Générer des audits de sécurité (SeAuditPrivilege).
- Remplacer un jeton de niveau processus (SeAssignPrimaryTokenPrivilege).

Ces trois privilèges ne doivent pas être retirés au compte (par GPO…), sous peine de ne plus pouvoir exécuter le service. Depuis Windows 2008 Server, il est cependant possible d'arrêter le service TSE, ce qui n'était pas le cas avant. Vous pouvez vérifier l'état actuel du service ainsi que les états acceptés par le service en utilisant la ligne de commande suivante :

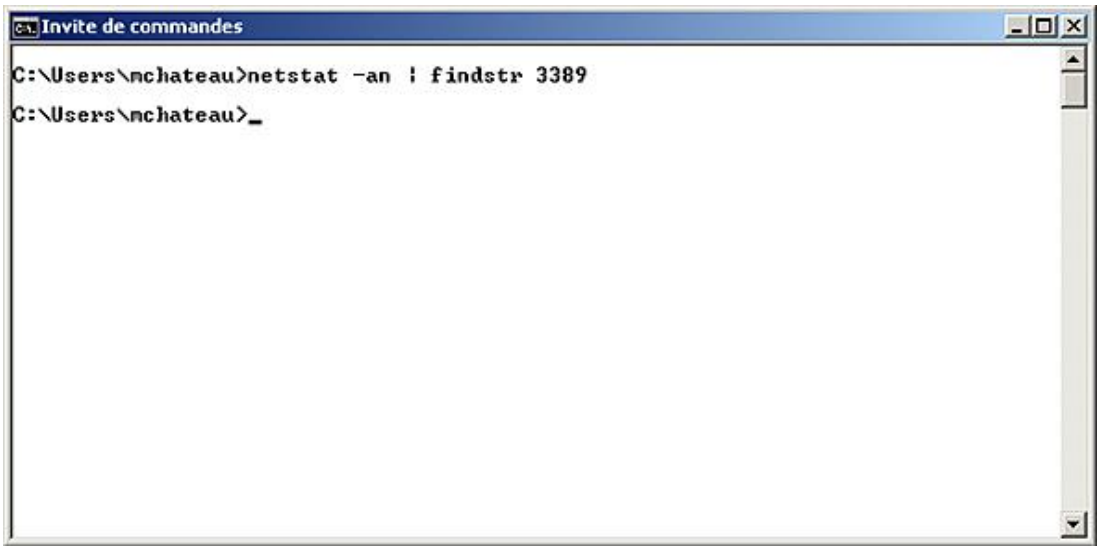
```
sc query TermService
```



Le service TSE utilise par défaut le port TCP 3389. Tant que l'accès à distance n'est pas autorisé explicitement, le service n'écoute pas le port TCP afin de ne pas exposer le service sur le réseau. La ligne de commande suivante permet de vérifier que le port TCP 3389 n'est pas écouté sur le serveur pour l'instant :

```
netstat -an | findstr 3389
```

© ENI Editions - All rigths reserved



Pour bénéficier de l'ensemble des fonctionnalités offertes par Windows Server 2008, le client RDP version 6.1 est nécessaire. Il est déjà inclus dans Windows Vista Service Pack 1 et Windows XP Service Pack 3. Si vous êtes sous Windows XP Service Pack 2, il est téléchargeable gratuitement à cette adresse : http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID= 6e1ec93d-bdbd-4983-92f7-479e088570ad

Les services de rôles qui composent le rôle sont :

- **Terminal Server** : permet à un serveur d'héberger des applications ou le bureau complet Windows. Les utilisateurs peuvent s'y connecter, et non plus seulement les administrateurs. La limitation à deux sessions concomitantes est levée.
- **Gestionnaire de licences** : gère l'attribution des licences CAL par périphérique ou utilisateur afin de se connecter à un serveur TS.
- **Session Broker TS** : permet la répartition des sessions TS dans une ferme de serveurs, ainsi que la reconnexion à une session existante dans une ferme.
- **Passerelle TS** : permet aux utilisateurs habilités de consommer des ressources depuis Internet du moment que le périphérique exécute le client RDC. Elle n'a pas vocation à remplacer un VPN, mais permet de s'en affranchir pour les accès aux ressources offertes par Terminal Services.
- **Accès Web TS** : permet aux utilisateurs d'accéder à des applications RemoteApp et au bureau à distance à travers un simple site Web. Un accès Web étant le minimum autorisé en général, cela permet de maximiser les possibilités d'accès par les utilisateurs, notamment depuis les hôtels ou d'autres entreprises.

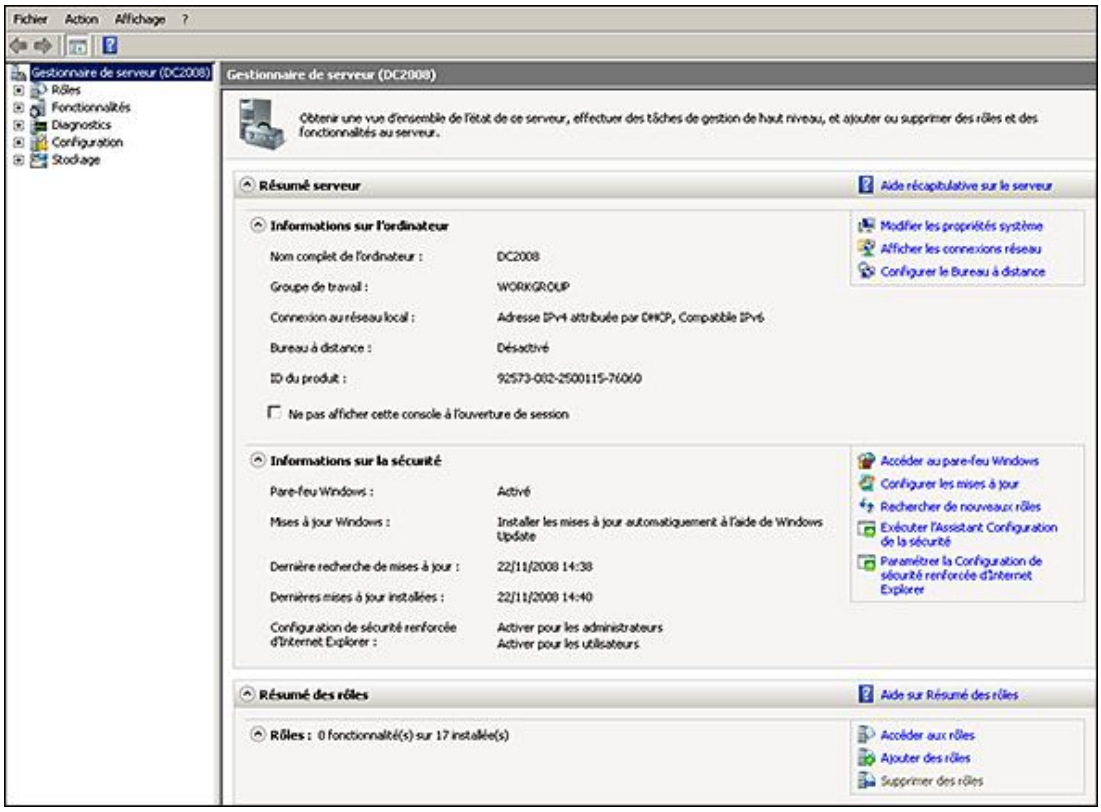
1. Administration à distance

Bien que le service Windows soit déjà installé et démarré, vous ne pouvez pas l'utiliser pour administrer à distance vos serveurs pour l'instant. Il faut autoriser explicitement l'accès à distance via le **Gestionnaire de serveur**.

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Gestionnaire de serveur**.

  Au niveau de **Résumé serveur**, cliquez sur **Configurer le Bureau à distance**.

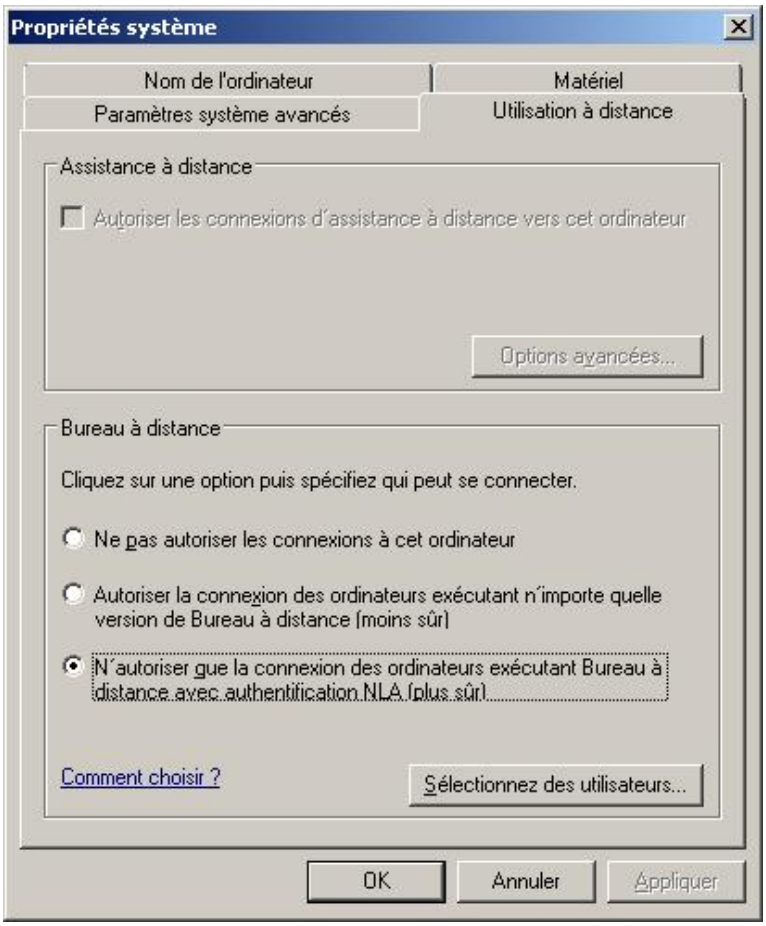
© ENI Editions - All rigths reserved


Fichier Action Affichage ?
Gestionnaire de serveur (DC2008)
Rôles
Fonctionnalités
Diagnostics
Configuration
Stockage
Gestionnaire de serveur (DC2008)
Obtenir une vue d'ensemble de l'état de ce serveur, effectuer des tâches de gestion de haut niveau, et ajouter ou supprimer des rôles et des fonctionnalités au serveur.
Résumé serveur
Aide récapitulative sur le serveur
Informations sur l'ordinateur
Nom complet de l'ordinateur : DC2008
Groupe de travail : WORKGROUP
Connexion au réseau local : Adresse IPv4 attribuée par DHCP, Compatible IPv6
Bureau à distance : Désactivé
ID du produit : 92573-002-2500115-76060
Ne pas afficher cette console à l'ouverture de session
Modifier les propriétés système
Afficher les connexions réseau
Configurer le Bureau à distance
Informations sur la sécurité
Pare-feu Windows : Activé
Mises à jour Windows : Installer les mises à jour automatiquement à l'aide de Windows Update
Dernière recherche de mises à jour : 22/11/2008 14:38
Dernières mises à jour installées : 22/11/2008 14:40
Configuration de sécurité renforcée d'Internet Explorer : Activer pour les administrateurs Activer pour les utilisateurs
Accéder au pare-feu Windows
Configurer les mises à jour
Rechercher de nouveaux rôles
Exécuter l'Assistant Configuration de la sécurité
Paramétrer la Configuration de sécurité renforcée d'Internet Explorer
Résumé des rôles
Aide sur Résumé des rôles
Rôles : 0 fonctionnalité(s) sur 17 installée(s)
Accéder aux rôles
Ajouter des rôles
Supprimer des rôles

- La fenêtre suivante s'affiche, permettant d'activer le bureau à distance, avec ou sans NLA. Choisissez **N'autoriser que la connexion des ordinateurs exécutant Bureau à distance avec authentification NLA (plus sûr)**.

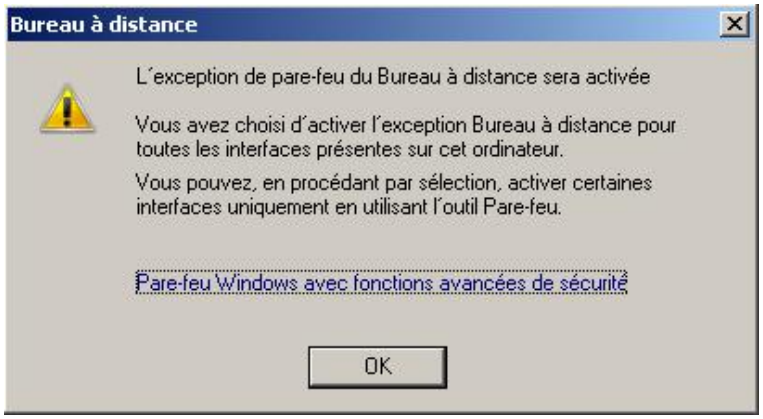
NLA signifie *Network Level Authentication*. L'objectif est de lutter contre les attaques dites de l'homme du milieu (man in the middle) en authentifiant le serveur TS avant que l'utilisateur ne s'y connecte. Il peut utiliser différents protocoles pour arriver à cet objectif : kerberos, TLS/SSL, NTLM. Techniquement, il s'appuie sur le fournisseur CredSSP qui utilise lui-même SSPI (*Security Service Provider Interface*). Après la phase d'authentification mutuelle, le client fournit les identifiants de l'utilisateur qui sont encryptés deux fois avec les clés de sessions SPNEGO et TLS.

© ENI Editions - All rigths reserved


Propriétés système
Nom de l'ordinateur
Matériel
Paramètres système avancés
Utilisation à distance
Assistance à distance
Autoriser les connexions d'assistance à distance vers cet ordinateur
Options avancées...
Bureau à distance
Cliquez sur une option puis spécifiez qui peut se connecter.
Ne pas autoriser les connexions à cet ordinateur
Autoriser la connexion des ordinateurs exécutant n'importe quelle version de Bureau à distance (moins sûr)
N'autoriser que la connexion des ordinateurs exécutant Bureau à distance avec authentification NLA (plus sûr)
Comment choisir ?
Sélectionnez des utilisateurs...
OK
Annuler
Appliquer

Cette interface modifie en fait deux clés de registre : **fDenyTSConnections** et **UserAuthentication**, situées sous **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server**. La première bloque toute connexion TS et la deuxième exige l'authentification NLA quand elles sont positionnées à 1.

- Le message d'information suivant apparaît, cliquez sur le bouton **OK**.

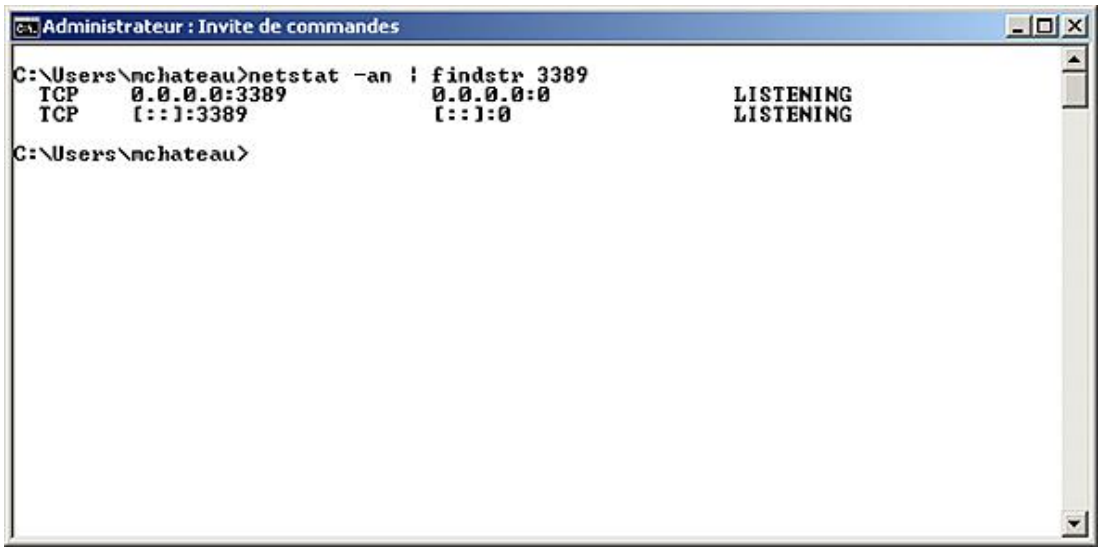

Bureau à distance
L'exception de pare-feu du Bureau à distance sera activée
Vous avez choisi d'activer l'exception Bureau à distance pour toutes les interfaces présentes sur cet ordinateur.
Vous pouvez, en procédant par sélection, activer certaines interfaces uniquement en utilisant l'outil Pare-feu.
Pare-feu Windows avec fonctions avancées de sécurité
OK

La gestion du pare-feu Windows est décrite dans le chapitre Sécuriser votre architecture.

- Cliquez sur le bouton **OK** pour fermer la fenêtre des propriétés système.

Maintenant que l'accès au bureau à distance est ouvert, le service TSE écoute le port TCP (une ligne pour IP version 4 et une ligne pour IP version 6) :

© ENI Editions - All rigths reserved



Pour la petite histoire, IPV5 existe bien, mais il s'agit d'une version de test (RFC 1819).

Vous pouvez maintenant utiliser le bureau à distance pour administrer votre serveur. Cette fonctionnalité n'a pas nécessité l'installation du rôle Terminal Service. L'administration à distance est jugée indispensable pour tous les serveurs, quel que soit leur usage, et ne caractérise donc pas un rôle à ce stade.

L'administration à distance est très utile, mais ne constitue pas une avancée notable. Il est donc temps d'exploiter tout le potentiel du rôle Terminal Services ! Pour cela, après avoir installé les composants du rôle, ils seront configurés dans le cadre d'un exemple concret.

2. Le rôle Terminal Services

a. Installation

Afin de ne pas s'installer dans la routine des assistants, installez le rôle et ses services associés avec l'outil **servermanagercmd**, depuis la ligne de commande :

```
servermanagercmd -i TS-Terminal-Server TS-Licensing TS-
Session-Broker TS-Gateway TS-Web-Access
```

Un message d'avertissement vous indiquera qu'un redémarrage est nécessaire pour prendre en compte l'installation du rôle. Si vous faîtes l'installation depuis le **gestionnaire de serveur**, et que le serveur a aussi le rôle contrôleur de domaine, une alerte vous indiquera que ce n'est pas recommandé. Installer le rôle TS sur un contrôleur de domaine comporte de vrais risques que vous devez évaluer au préalable.

Redémarrez le serveur pour finaliser l'installation de ce rôle. Une icône dans la barre des tâches vous alertera sur l'absence de licences. Faute d'avoir un serveur de licences TSE, un délai de grâce de 120 jours sera mis en œuvre. Vérifiez que les services de rôles sont bien installés, depuis la ligne de commande avec :

```
servermanagercmd -q | findstr TS
```

© ENI Editions - All rigths reserved

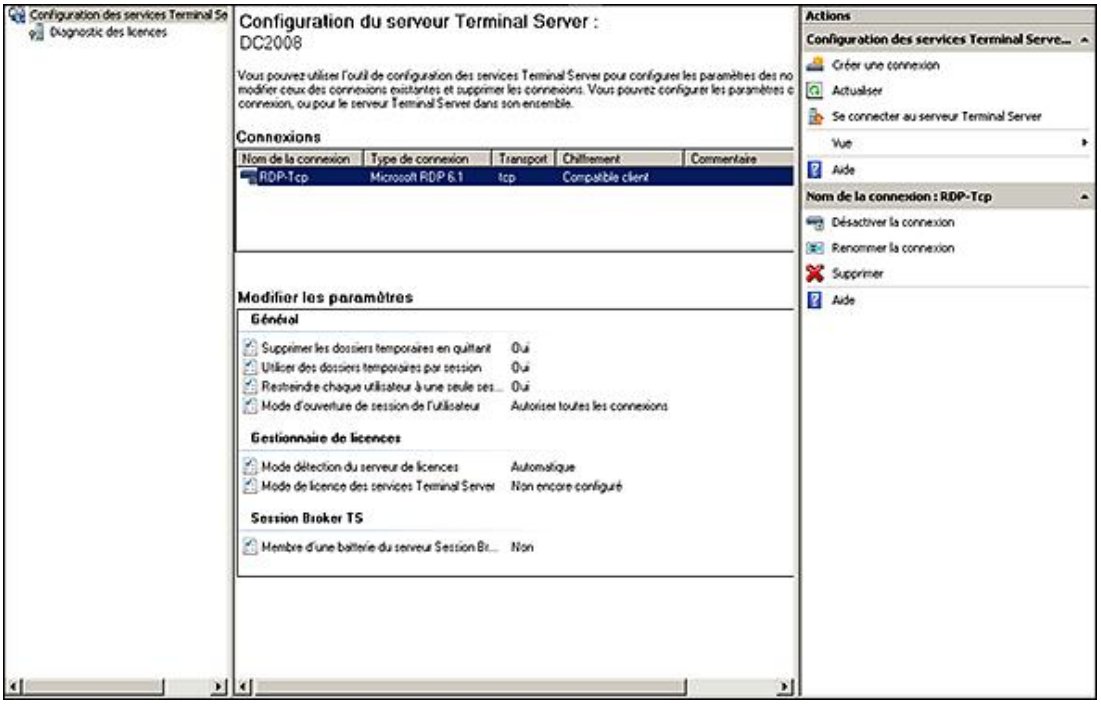
Administrateur : Invite de commandes
C:\Users\mchateau>servermanagercmd -q | findstr TS
[X] Terminal Server [TS-Terminal-Server]
[X] Gestionnaire de licences TS [TS-Licensing]
[X] Session Broker TS [TS-Session-Broker]
[X] Passerelle TS [TS-Gateway]
[X] Accès Web TS [TS-Web-Access]
[ ] Extensions du serveur BITS [BITS]
[X] Outils des services Terminal Server [RSAT-TS]
[X] Outils du serveur Terminal Server [RSAT-TS-RemoteApp]
[X] Outils de la passerelle TS [RSAT-TS-Gateway]
[X] Outils des licences Terminal Server [RSAT-TS-Licensing]
[ ] Outils d'extensions du serveur BITS [RSAT-Bits-Server]
C:\Users\mchateau>

Dans cet exemple, l'ensemble des rôles sont sur un serveur unique. Cependant, dans votre architecture, il peut être pertinent d'installer par exemple le **Gestionnaire de Licences TS** sur le serveur exécutant KMS (*Key Management System*). Si ce service de rôle est en particulier installé sur un contrôleur de domaine, tous les serveurs TS du domaine seront capables de le trouver automatiquement.

b. Configuration

La configuration se fait via la console **tsadmin.msc**. Vous pouvez la lancer depuis le menu **démarrer** :

- Ouvrez la console **Configuration des services Terminal Server** en cliquant sur le bouton **Démarrer**, **Outils d'administration**, puis **Services Terminal Server** et enfin **Configuration des services Terminal Server**.



- Cliquez deux fois sur la connexion **RDP-Tcp**.

Depuis l'onglet **Sessions**, vous pouvez définir la durée de vie des sessions inactives, ainsi que le comportement à adopter quand le temps imparti est atteint. Pourquoi gérer ses aspects ? Si un utilisateur ne fait que se déconnecter, toute sa session ainsi que les programmes en mémoire restent sur le serveur. La consommation en ressource système étant toujours présente, le serveur ne peut pas accueillir d'autres utilisateurs à la place. Voici une explication et une recommandation des paramètres :

- **Fin d'une session déconnectée** : ferme de façon arbitraire toute session déconnectée. Valeur suggérée : 2 heures.

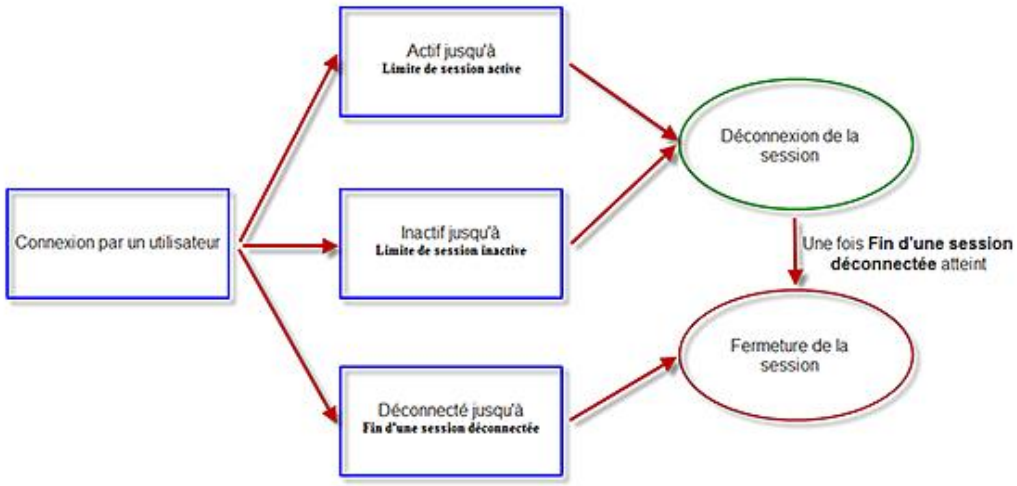
© ENI Editions - All rigths reserved

- **Limite de session active** : oblige l'utilisateur à fermer sa session même s'il est actif. Cela permet de lutter contre les fuites mémoires dans les applications, et éviter qu'un utilisateur ne ferme jamais sa session. Valeur suggérée : 12 heures.

- **Limite de session inactive** : ferme de façon arbitraire toute session maintenue par un client, mais qui n'envoie pas d'évènements clavier/souris. Valeur suggérée : 4 heures.

- **Lorsque la limite de session est atteinte ou la connexion est interrompue** : action à appliquer quand un des deux évènements est atteint. Choix suggéré : **Déconnexion de la session**.

L'enchaînement est donc le suivant :



Le temps maximum avant la fermeture d'une session est donc égal à :

Limite de session active + **Fin d'une session déconnectée** = 14 heures.

Vous avez remarqué que l'utilisateur a encore 2 heures potentielles pour se reconnecter sans perdre pour autant sa session.

Avant de sauvegarder un serveur TS le soir, il est recommandé de fermer toutes les sessions TS du serveur de façon arbitraire. Cela évite les erreurs sur les fichiers ouverts en mode exclusif, et permet de sauvegarder les profils TSE (recopiés à la fermeture de session sur leur répertoire).

---

c. Configuration de l'accès Web TS

L'usage de Terminal Services s'est étendu bien au-delà d'un simple bureau à distance. Windows Server 2008 offre donc un moyen pour centraliser les ressources publiées sur un portail Web. Du point de vue client, deux critères restent nécessaires :

- Pouvoir accéder au site Web fourni par l'accès Web TS, depuis un navigateur, avec ou sans proxy.

- Avoir le client RDC 6.1 installé. Il est déjà intégré à Windows depuis Windows Vista Service Pack 1 et Windows XP Service Pack 3.

Ce service de rôle peut être installé sur un serveur qui n'a pas le service Terminal Server. Il nécessite toutefois IIS 7 pour fonctionner, et une relation de confiance avec les serveurs Terminal Server pour pouvoir lister les applications RemoteApp.

Pour accéder au service, ouvrez un navigateur Web à cette adresse, en remplaçant *MonServeurWebTS* par le nom du serveur ayant le service de rôle : http://MonServeurWebTS/ts/fr-FR/default.aspx

© ENI Editions - All rigths reserved

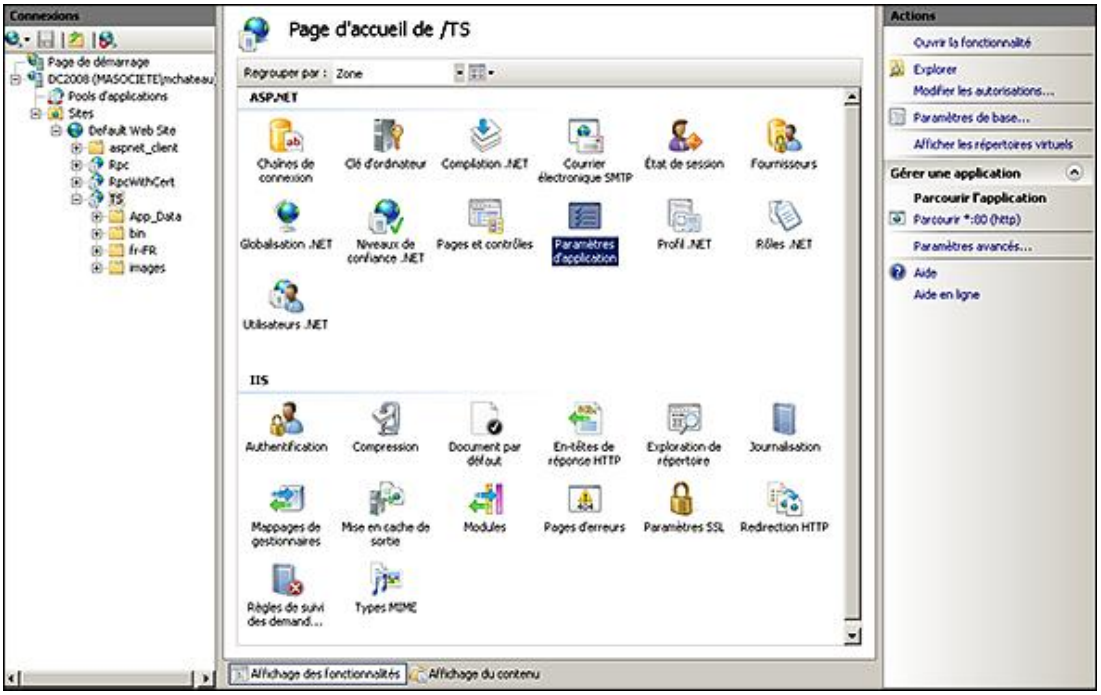
Deux onglets sont présents. L'onglet **Programmes RemoteApp** est peuplé dynamiquement des applications auxquelles vous avez droit si la fonctionnalité RemoteApp a été configurée. L'onglet **Bureau à distance** permet d'avoir une session RDP complète via le site Web.

L'onglet **Bureau à distance** offre quelques options, mais ne permet pas de choisir le serveur sur lequel ouvrir une connexion. Pour configurer le service, vous avez deux options possibles :

- passer par la MMC IIS7 ;
- éditer le fichier de configuration XML, *web.config*, présent par défaut dans C:\Windows\Web\TS.

Configuration via IIS :

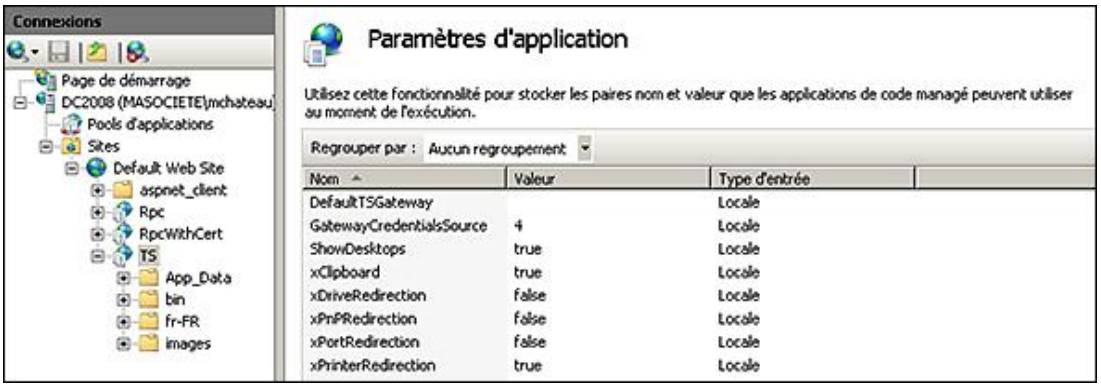
- Ouvrez la console **Gestionnaire des services Internet (IIS)** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Gestionnaire des services Internet (IIS)**.
- Dans l'onglet **Connexions**, dépliez le nom de votre serveur, puis **Sites - Default Web Site** et enfin le dossier virtuel **TS**.
- Cliquez deux fois sur l'icône **Paramètres d'application** au centre de l'écran :



Le site d'accès Web TS peut être incorporé dans un site SharePoint, car il s'agit d'un web part. Cette partie n'est pas couverte dans cet ouvrage, car SharePoint est hors périmètre.

Les paramètres configurables sont les suivants :

© ENI Editions - All rigths reserved



DefaultTSGateway : permet de spécifier la passerelle par défaut à utiliser pour les connexions. Par défaut, aucune passerelle n'est positionnée. Une fois l'application RemoteApp ou le bureau à distance choisi, une connexion RDP classique sur le port TCP 3389 sera effectuée.

GatewayCredentialsSource : peut prendre les valeurs 0, 1 ou 4. La valeur par défaut est 4, ce qui correspond à « me demander plus tard ».

ShowDesktops : positionné à *true* par défaut. Cette variable contrôle le fait d'afficher ou non l'onglet **Bureau à distance** sur le site Web.

xClipboard : positionné à *true* par défaut. Bloque l'utilisation du presse papier Windows s'il est positionné à *false*.

xDriveRedirection : positionné à *false* par défaut. Autorise la redirection des lecteurs locaux s'il est positionné à *true*.

xPnPRedirection : positionné à *false* par défaut. Autorise la redirection de périphériques dit plug & play s'il est positionné à *true*. Cela concerne uniquement les périphériques multimédia prenant en charge le *Media Transfer Protocol*, le *Picture Transfer Protocol* ou *Microsoft Point of Service (POS) for .NET 1.11*.

xPortRedirection : positionné à *false* par défaut. Autorise la redirection de port COM et LPT s'il est positionné à *true*.

xPrinterRedirection : positionné à *true* par défaut. Bloque la redirection des imprimantes s'il est positionné à *false*.

Passer par le fichier XML web.config a l'avantage de montrer les commentaires qui expliquent les différentes valeurs, par exemple pour GatewayCredentialsSource :

```
<!-- GatewayCredentialsSource: TS Gateway Authentication Type.
          Admins can preset this.
          0 = User Password
          1 = Smartcard
          4 = "Ask me later"
-->
```

Les modifications sont prises à chaud et ne nécessitent aucun redémarrage. Il suffit de rafraîchir la page Web pour voir les changements.

Si l'accès Web TS est installé sur un serveur qui est aussi Terminal Server, il utilisera le serveur où il est installé pour détecter les applications publiées via RemoteApp. En revanche, s'il est installé seul, l'onglet supplémentaire **Configuration** permettra de choisir le serveur TS à partir duquel afficher les applications publiées. Le groupe Windows *Ordinateurs Accès Web TS* devra contenir le compte ordinateur du serveur d'accès Web TS, afin qu'il puisse interroger la liste des programmes.

Dans notre cas, tous les services de rôles sont sur le même serveur. Mais ajouter le serveur à ce groupe est recommandé afin d'être conforme. Comme il s'agit d'un contrôleur de domaine, il faut éditer le groupe *Ordinateurs Accès Web TS* via le composant *DSA* : **Démarrer - Exécuter - dsa.msc**. La seule particularité est qu'il faut ajouter les objets ordinateurs dans les filtres.

Par défaut, les applications RemoteApp sont activées pour l'Accès Web TS. Cette autorisation peut se gérer par application, depuis la console **Gestionnaire RemoteApp TS**.

d. Configuration de la passerelle TS

L'usage de Terminal Service s'est répandu au-delà des frontières de l'entreprise. Une fois en dehors de l'entreprise, on ne maîtrise plus l'infrastructure en place, ainsi que leur restriction. Ouvrir une connexion sur le port TCP 3389 depuis une autre société, un hôtel ou autre est parfois bloqué par des firewalls, ce qui limite la pertinence de TS. Windows Server 2008 offre donc un moyen de transport adapté à ce contexte pour accéder aux ressources TS :

© ENI Editions - All rigths reserved

HTTPS.

Le premier pré-requis sera d'avoir un certificat SSL valide, que ce soit via un tiers de confiance, soit via votre propre infrastructure de PKI. Windows Server 2008 vous permet de générer un certificat auto-signé, mais cela implique de pouvoir ajouter ce certificat racine sur les ordinateurs utilisés pour se connecter. Cette solution est peu onéreuse, mais l'expérience utilisateur n'est pas optimale, et va être problématique pour se connecter depuis un ordinateur en libre service dans un hôtel, par exemple. Le principal étant que le poste client considère votre certificat comme digne de confiance.

Les attributs du certificat doivent respecter certaines règles que voici :

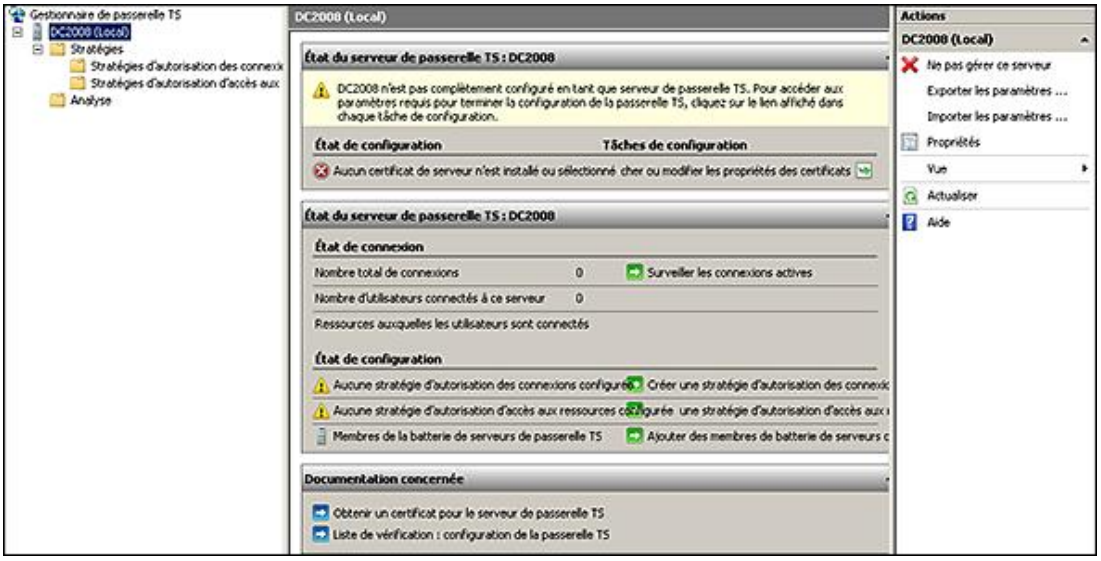
- Le certificat doit être de type ordinateur.
- L'objet du certificat est l'authentification du serveur. L'attribut EKU est de type Server Authentication (1.3.6.1.5.5.7.3.1).
- Le certificat ne doit pas être expiré.
- Un OID de 2.5.29.15 n'est pas requis, mais si vous souhaitez l'utiliser il doit aussi avoir un de ces usages :

  CERT_KEY_ENCIPHERMENT_KEY_USAGE, CERT_KEY_AGREEMENT_KEY_USAGE,

  et CERT_DATA_ENCIPHERMENT_KEY_USAGE.
- Le nom du certificat (CN) doit correspondre au nom DNS utilisé par le client pour se connecter à la passerelle.

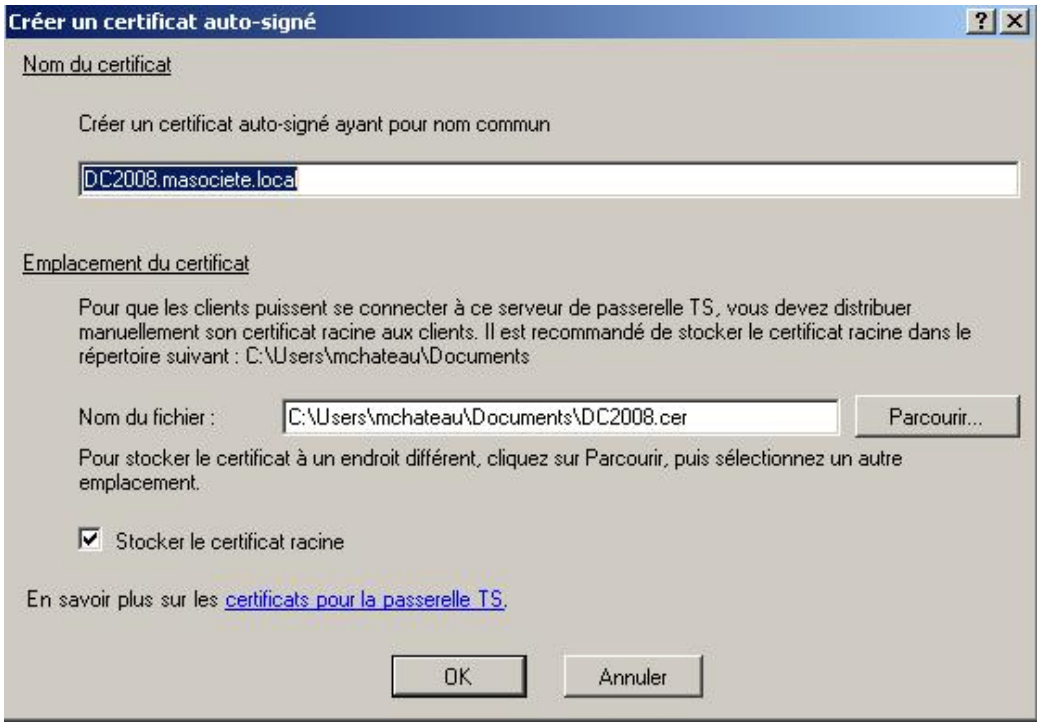
Pour créer un certificat :

- Ouvrez la console **Gestionnaire de passerelle TS** en cliquant sur le bouton **Démarrer**, **Outils d'administration**, **Services Terminal Server** puis **Gestionnaire de passerelle TS**.


Gestionnaire de passerelle TS
DC2008 (Local)
Stratégies
Stratégies d'autorisation des connexi
Stratégies d'autorisation d'accès aux
Analyse
DC2008 (Local)
État du serveur de passerelle TS : DC2008
DC2008 n'est pas complètement configuré en tant que serveur de passerelle TS. Pour accéder aux paramètres requis pour terminer la configuration de la passerelle TS, cliquez sur le lien affiché dans chaque tâche de configuration.
État de configuration
Tâches de configuration
Aucun certificat de serveur n'est installé ou sélectionné cher ou modifier les propriétés des certificats
État du serveur de passerelle TS : DC2008
État de connexion
Nombre total de connexions 0
Surveiller les connexions actives
Nombre d'utilisateurs connectés à ce serveur 0
Ressources auxquelles les utilisateurs sont connectés
État de configuration
Aucune stratégie d'autorisation des connexions configurée
Créer une stratégie d'autorisation des connexi
Aucune stratégie d'autorisation d'accès aux ressources configurée une stratégie d'autorisation d'accès aux
Membres de la batterie de serveurs de passerelle TS
Ajouter des membres de batterie de serveurs
Documentation concernée
Obtenir un certificat pour le serveur de passerelle TS
Liste de vérification : configuration de la passerelle TS
Actions
DC2008 (Local)
Ne pas gérer ce serveur
Exporter les paramètres ...
Importer les paramètres ...
Propriétés
Vue
Actualiser
Aide

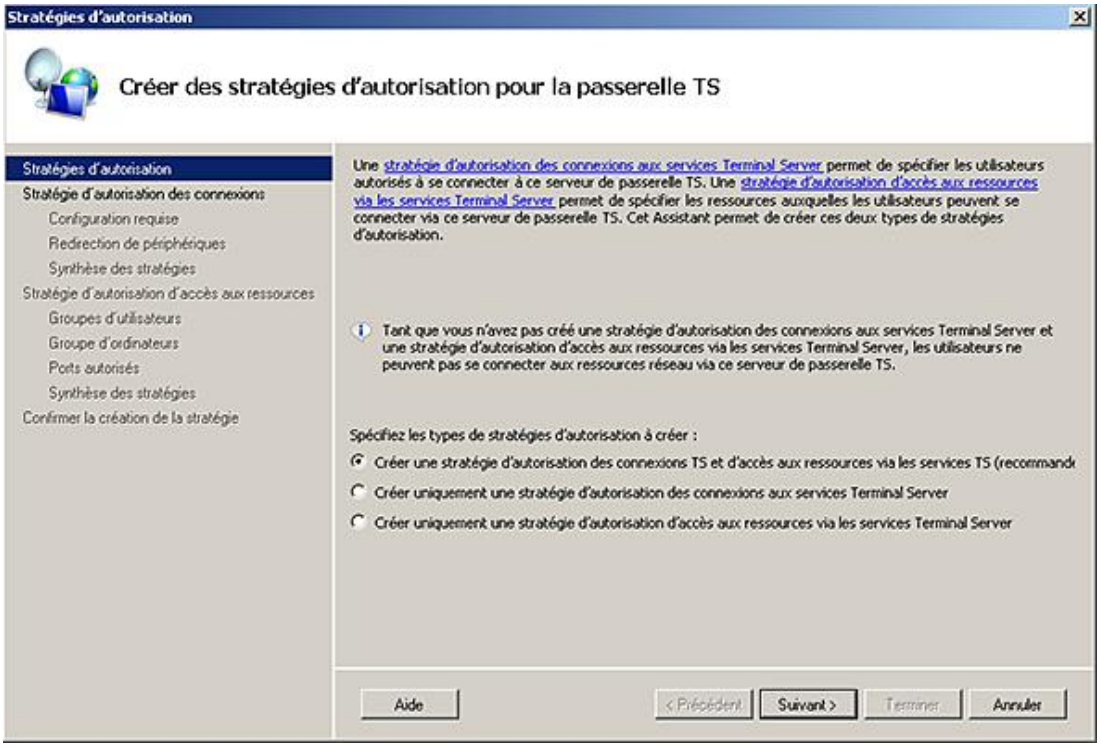
- Dans le panneau gauche, faites un clic avec le bouton droit sur le nom de votre serveur, puis cliquez sur **Propriétés**.
- Dans l'onglet **Certificat SSL**, cliquez sur **Créer un certificat**. L'écran suivant apparaît :

© ENI Editions - All rigths reserved


Créer un certificat auto-signé
Nom du certificat
Créer un certificat auto-signé ayant pour nom commun
DC2008.masociete.local
Emplacement du certificat
Pour que les clients puissent se connecter à ce serveur de passerelle TS, vous devez distribuer manuellement son certificat racine aux clients. Il est recommandé de stocker le certificat racine dans le répertoire suivant : C:\Users\mchateau\Documents
Nom du fichier :
C:\Users\mchateau\Documents\DC2008.cer
Parcourir...
Pour stocker le certificat à un endroit différent, cliquez sur Parcourir, puis sélectionnez un autre emplacement.
Stocker le certificat racine
En savoir plus sur les certificats pour la passerelle TS.
OK
Annuler

Il faudra ajouter le certificat racine généré à tous les clients utilisant la passerelle. Cela permet d'avoir tout de suite la passerelle TS qui fonctionne sans message d'avertissement, mais cela n'est pas souhaitable en production. Il est toutefois suffisant dans le cadre de cet ouvrage.

- Validez le message d'information, et revenez à la fenêtre principale du Gestionnaire de passerelle TS.
- Dépliez le dossier **Stratégies**, puis cliquez sur **Créer des stratégies d'autorisation pour la passerelle TS**.


Stratégies d'autorisation
Créer des stratégies d'autorisation pour la passerelle TS
Stratégies d'autorisation
Stratégie d'autorisation des connexions
Configuration requise
Redirection de périphériques
Synthèse des stratégies
Stratégie d'autorisation d'accès aux ressources
Groupes d'utilisateurs
Groupe d'ordinateurs
Ports autorisés
Synthèse des stratégies
Confirmer la création de la stratégie
Une stratégie d'autorisation des connexions aux services Terminal Server permet de spécifier les utilisateurs autorisés à se connecter à ce serveur de passerelle TS. Une stratégie d'autorisation d'accès aux ressources via les services Terminal Server permet de spécifier les ressources auxquelles les utilisateurs peuvent se connecter via ce serveur de passerelle TS. Cet Assistant permet de créer ces deux types de stratégies d'autorisation.
Tant que vous n'avez pas créé une stratégie d'autorisation des connexions aux services Terminal Server et une stratégie d'autorisation d'accès aux ressources via les services Terminal Server, les utilisateurs ne peuvent pas se connecter aux ressources réseau via ce serveur de passerelle TS.
Spécifiez les types de stratégies d'autorisation à créer :
Créer une stratégie d'autorisation des connexions TS et d'accès aux ressources via les services TS (recommandé)
Créer uniquement une stratégie d'autorisation des connexions aux services Terminal Server
Créer uniquement une stratégie d'autorisation d'accès aux ressources via les services Terminal Server
Aide
< Précédent
Suivant >
Terminer
Annuler

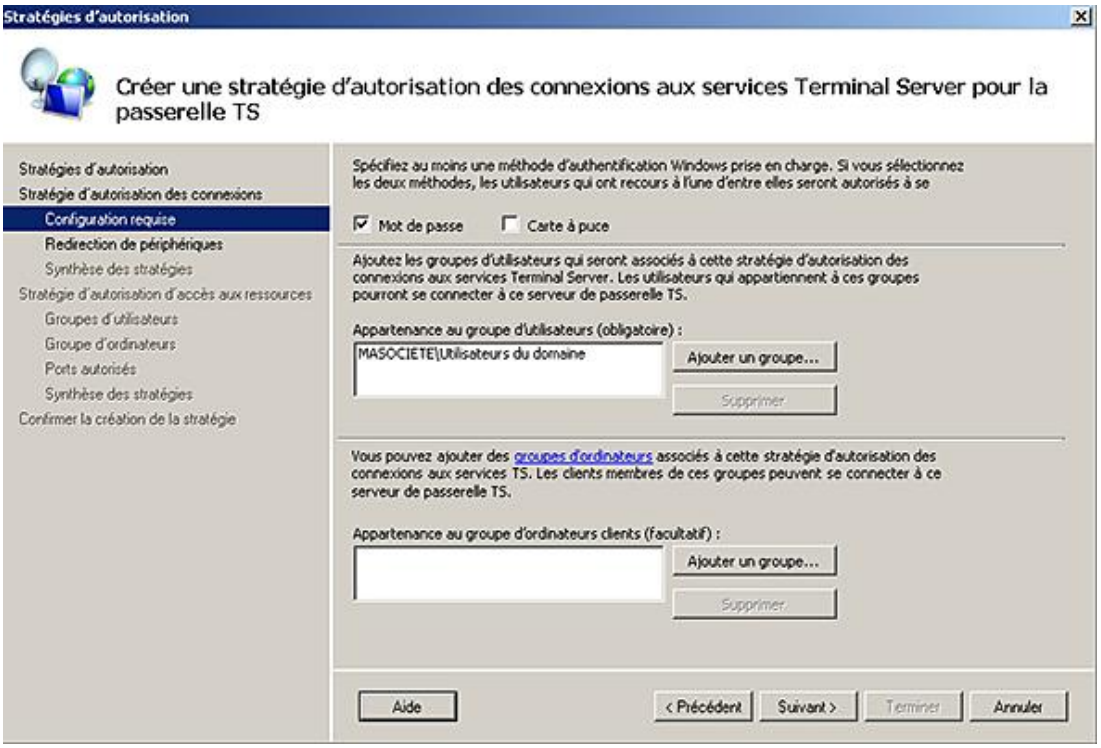
- Choisissez **Créer une stratégie d'autorisation des connexions TS et d'accès aux ressources via les services TS (recommandé)** puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved

- Choisissez un nom à donner à la stratégie, *Stratégie des connexions de masociete* par exemple.

- L'écran suivant vous permet de définir les méthodes d'authentification acceptées (mot de passe, carte à puce ou les deux). Vous devez ensuite spécifier les groupes d'utilisateurs et d'ordinateurs autorisés à utiliser la passerelle.

- Ajoutez le groupe *Utilisateurs du domaine* pour **Appartenance au groupe d'utilisateurs** puis cliquez sur **Suivant**.


Stratégies d'autorisation
Créer une stratégie d'autorisation des connexions aux services Terminal Server pour la passerelle TS
Stratégies d'autorisation
Stratégie d'autorisation des connexions
Configuration requise
Redirection de périphériques
Synthèse des stratégies
Stratégie d'autorisation d'accès aux ressources
Groupes d'utilisateurs
Groupe d'ordinateurs
Ports autorisés
Synthèse des stratégies
Confirmer la création de la stratégie
Spécifiez au moins une méthode d'authentification Windows prise en charge. Si vous sélectionnez les deux méthodes, les utilisateurs qui ont recours à l'une d'entre elles seront autorisés à se
Mot de passe
Carte à puce
Ajoutez les groupes d'utilisateurs qui seront associés à cette stratégie d'autorisation des connexions aux services Terminal Server. Les utilisateurs qui appartiennent à ces groupes pourront se connecter à ce serveur de passerelle TS.
Appartenance au groupe d'utilisateurs (obligatoire) :
MASOCIETE\Utilisateurs du domaine
Ajouter un groupe...
Supprimer
Vous pouvez ajouter des groupes d'ordinateurs associés à cette stratégie d'autorisation des connexions aux services TS. Les clients membres de ces groupes peuvent se connecter à ce serveur de passerelle TS.
Appartenance au groupe d'ordinateurs clients (facultatif) :
Ajouter un groupe...
Supprimer
Aide
< Précédent
Suivant >
Terminer
Annuler

- Par défaut, l'ensemble des redirections sont actives via la passerelle. Vous avez la possibilité de restreindre les redirections disponibles. Cliquez sur **Suivant**.

- La synthèse de la stratégie vous est affichée, cliquez sur **Suivant**.

- L'assistant permet maintenant de créer une **Stratégie d'autorisation d'accès aux ressources**. Entrez *Stratégie d'accès aux ressources de masociété* comme nom et cliquez sur **Suivant**.

- Le groupe d'utilisateurs autorisés à accéder aux ressources est déjà prérempli avec le groupe déclaré pour la première stratégie. Cliquez sur **Suivant**.

- Il est important de définir les ordinateurs auxquels les utilisateurs pourront accéder à travers la passerelle. Il est possible de spécifier un groupe Active Directory, un groupe géré par la passerelle TS ou bien tous les ordinateurs. En production, vous devriez être le plus restrictif possible dans l'ouverture des accès. Choisissez **Autoriser les utilisateurs à se connecter à n'importe quelle ressource réseau (ordinateur)** et cliquez sur **Suivant**.

- L'écran suivant permet de définir les ports réseaux autorisés. Par défaut, seul le port TCP 3389, qui est le port RDP par défaut est autorisé. Cliquez sur **Suivant**.

- La synthèse de la stratégie s'affiche, cliquez sur **Suivant** puis sur **Fermer**.

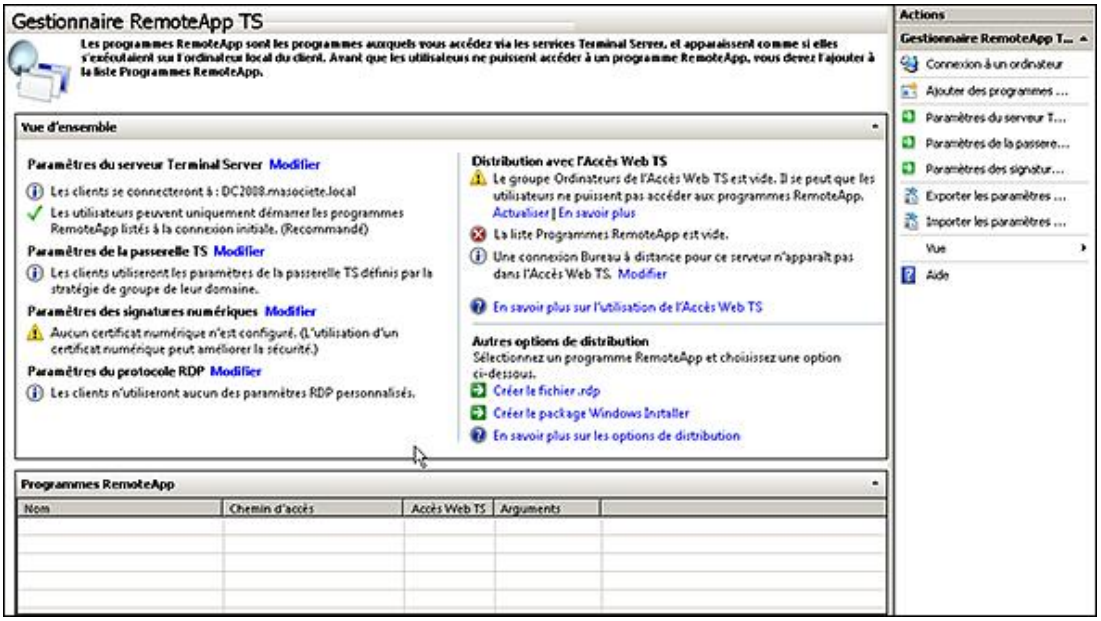
La passerelle TS est maintenant opérationnelle. Elle possède un certificat SSL auto généré et deux stratégies ont été définies. Tous les utilisateurs du domaine peuvent utiliser la passerelle pour accéder à n'importe quel ordinateur du réseau.

e. Configuration du RemoteApp

Ce service de rôle rend Terminal Service très attrayant. Il permet de publier des applications au lieu d'un bureau complet. Pour le configurer :

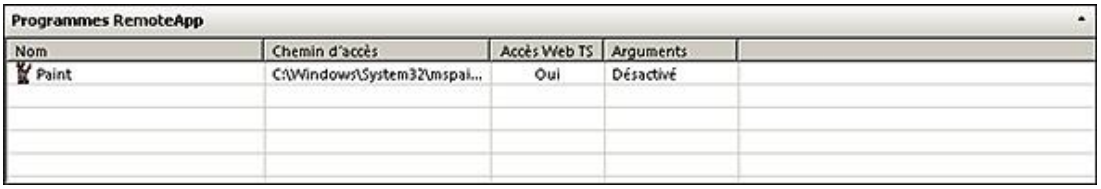
© ENI Editions - All rigths reserved

- Ouvrez la console **Gestionnaire RemoteApp TS** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Services Terminal Server** et **Gestionnaire RemoteApp TS**.


Gestionnaire RemoteApp TS
Les programmes RemoteApp sont les programmes auxquels vous accédez via les services Terminal Server, et apparaissent comme si elles s'exécutaient sur l'ordinateur local du client. Avant que les utilisateurs ne puissent accéder à un programme RemoteApp, vous devez l'ajouter à la liste Programmes RemoteApp.
Vue d'ensemble
Paramètres du serveur Terminal Server Modifier
Les clients se connecteront à : DC2008.masociete.local
Les utilisateurs peuvent uniquement démarrer les programmes RemoteApp listés à la connexion initiale. (Recommandé)
Paramètres de la passerelle TS Modifier
Les clients utiliseront les paramètres de la passerelle TS définis par la stratégie de groupe de leur domaine.
Paramètres des signatures numériques Modifier
Aucun certificat numérique n'est configuré. (L'utilisation d'un certificat numérique peut améliorer la sécurité.)
Paramètres du protocole RDP Modifier
Les clients n'utiliseront aucun des paramètres RDP personnalisés.
Distribution avec l'Accès Web TS
Le groupe Ordinateurs de l'Accès Web TS est vide. Il se peut que les utilisateurs ne puissent pas accéder aux programmes RemoteApp.
Actualiser | En savoir plus
La liste Programmes RemoteApp est vide.
Une connexion Bureau à distance pour ce serveur n'apparaît pas dans l'Accès Web TS. Modifier
En savoir plus sur l'utilisation de l'Accès Web TS
Autres options de distribution
Sélectionnez un programme RemoteApp et choisissez une option ci-dessous.
Créer le fichier .rdp
Créer le package Windows Installer
En savoir plus sur les options de distribution
Programmes RemoteApp
Nom
Chemin d'accès
Accès Web TS
Arguments
Actions
Gestionnaire RemoteApp T...
Connexion à un ordinateur
Ajouter des programmes ...
Paramètres du serveur T...
Paramètres de la passere...
Paramètres des signatur...
Exporter les paramètres ...
Importer les paramètres ...
Vue
Aide

Par défaut, l'accès bureau à distance n'apparaît pas pour notre serveur sur l'accès Web TS configuré précédemment. Les utilisateurs peuvent toujours aller dans l'onglet **Bureau à distance** et renseigner le nom du serveur, mais ce n'est pas très ergonomique. Pour ajouter explicitement une icône bureau à distance dans les RemoteApp, cliquez sur un des hypertextes **Modifier**. Allez dans l'onglet **Terminal Server** et cochez la case **Afficher une connexion Bureau à distance avec ce serveur Terminal Server dans l'Accès Web TS**.

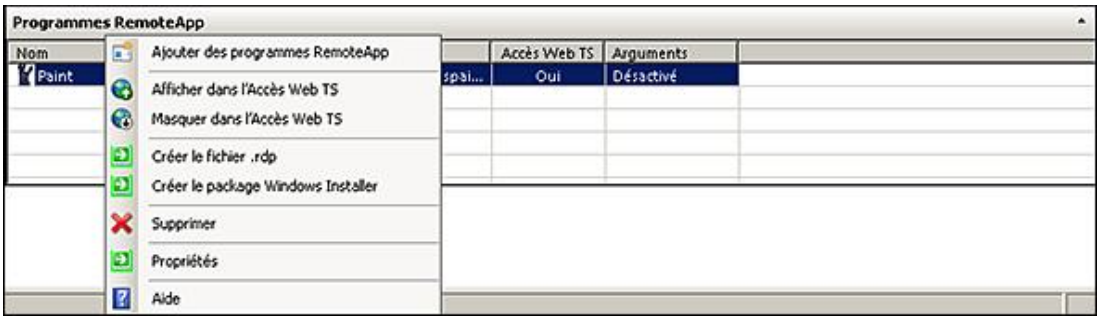
Pour publier un programme via RemoteApp, dans le panneau droit **Actions**, cliquez sur **Ajouter des programmes**. Cliquez sur **Suivant**, puis choisissez **Paint** et cliquez sur **Suivant** et **Terminer**. L'application Paint apparaît maintenant dans la liste des programmes RemoteApp :



Depuis l'Accès Web TS, l'application apparaît immédiatement en rafraîchissant l'écran :

RemoteApp permet aussi de créer un fichier rdp ou un package Windows Installer afin que les utilisateurs puissent accéder à l'application :

© ENI Editions - All rigths reserved



- Le fichier rdp est très simple à déployer et peut être envoyé par mail aux utilisateurs.

- L'installation via un package MSI complique l'installation, mais permet un inventaire sur les postes de travail, une industrialisation du déploiement, ainsi qu'associer les extensions de fichiers. Par exemple, si Microsoft Visio est uniquement disponible via Terminal Service, le package peut associer l'extension .vsd à cette application publiée. Ainsi, lorsqu'un utilisateur double clique sur un fichier .vsd, Microsoft Visio est automatiquement lancé en tant que RemoteApp et ouvre le fichier demandé. L'opération est donc transparente pour l'utilisateur.

f. Configuration du gestionnaire de licences TS

Les licences TS sont proposées sous deux types :

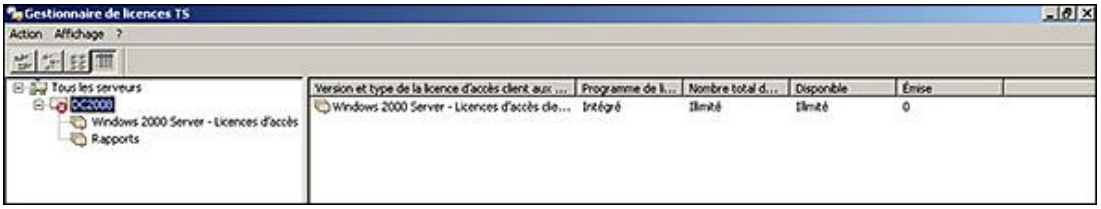
- par périphérique, quel que soit le nombre d'utilisateurs utilisant ce périphérique pour accéder à des ressources TS ;

- par utilisateur, quel que soit le périphérique utilisé pour accéder à des ressources TS.

Il est recommandé d'installer ce service rôle sur un contrôleur de domaine, car tous les serveurs TS du domaine trouveront automatiquement le serveur de licence.

Pour configurer le service de licences TS, lancez la console de gestion :

- Ouvrez la console **Gestionnaire de licences TS** en cliquant sur le bouton **Démarrer**, **Outils d'administration**, puis **Services Terminal Server** et **Gestionnaire de licences TS**.



La première étape va consister à activer le serveur auprès de Microsoft. Trois méthodes sont possibles :

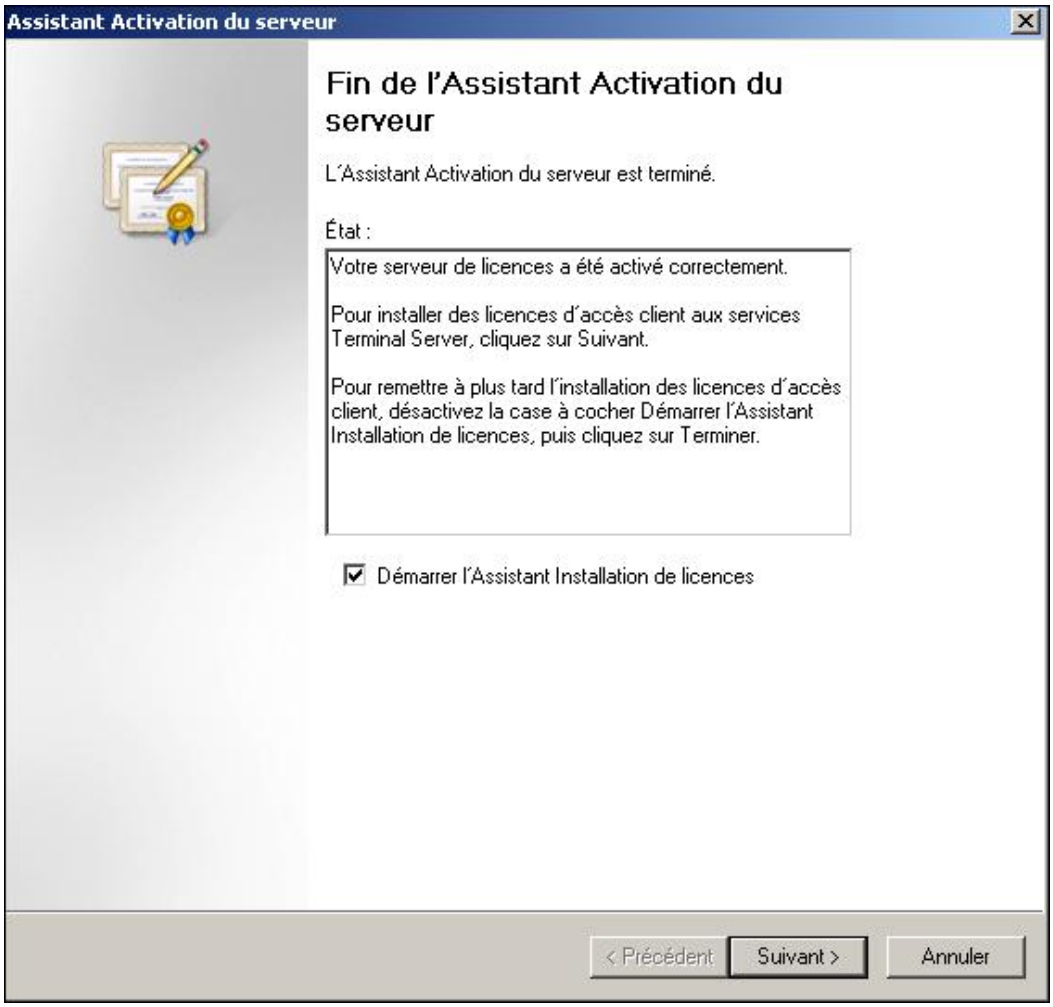
- **Connexion automatique**. Le serveur doit pouvoir établir une connexion au serveur Microsoft via le protocole https.

- **Navigateur Web**. Utilisez un autre ordinateur qui lui a accès à Internet pour faire la procédure d'activation.

- **Par téléphone**. Vous allez échanger des numéros de série avec Microsoft par téléphone.

- Pour ce faire, faites un clic avec le bouton droit sur le nom du serveur et cliquez sur **Activer le serveur**. Une fois l'activation effectuée, vous aurez cet écran :

© ENI Editions - All rigths reserved


Assistant Activation du serveur
Fin de l'Assistant Activation du serveur
L'Assistant Activation du serveur est terminé.
État :
Votre serveur de licences a été activé correctement.
Pour installer des licences d'accès client aux services Terminal Server, cliquez sur Suivant.
Pour remettre à plus tard l'installation des licences d'accès client, désactivez la case à cocher Démarrer l'Assistant Installation de licences, puis cliquez sur Terminer.
Démarrer l'Assistant Installation de licences
< Précédent
Suivant >
Annuler

Cela ne constitue que la première étape, enregistrer votre serveur auprès de Microsoft. Maintenant il est possible d'ajouter des licences TS, en choisissant le programme de licences. Une fois que vous aurez fourni les numéros nécessaires, les licences TS seront affichées dans le **Gestionnaire de licences TS**.

- Ce Service de rôle consomme très peu de ressource, mais doit être mis sur un serveur stable. Les licences ne pourront pas être transférées sur un autre serveur facilement, et l'absence de ce rôle passe l'ensemble des serveurs TS en période de grâce de 120 jours.

- Un serveur TS Windows 2008 Server peut uniquement communiquer avec un serveur de licences TS Windows 2008 Server.

- Par défaut, une base de données des licences TS est créée sur le serveur dans ce répertoire : %systemroot%\system32\lserver.

- Lors de l'installation, le service de licence TS a créé un groupe, *Terminal Server Computers*. Ce groupe est local, sauf s'il est installé sur un contrôleur de domaine, auquel cas cela devient un groupe Active Directory. Si la GPO Computer *Configuration\Administrative Templates\Windows Components\Terminal Services\TS Licensing\License server security group* est activée, seuls les ordinateurs membres du groupe pourront interroger le service de licence TS.

- Le gestionnaire de Licences TS permet de suivre la consommation des licences en mode utilisateur, et de générer des rapports. Pour utiliser cette fonctionnalité, l'objet ordinateur du serveur doit être membre du groupe AD **Serveurs de licences des services Terminal Server**. Si le serveur est aussi un contrôleur de domaine, le compte Service Réseau doit aussi être membre de ce groupe.

- S'il n'est pas installé sur un contrôleur de domaine, vous pouvez spécifier manuellement le nom du serveur de licences TS sur les serveurs TS via la base de registre. Il faut créer la clé DefaultLicenseServer de type REG_SZ avec le nom du serveur dans :

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters.

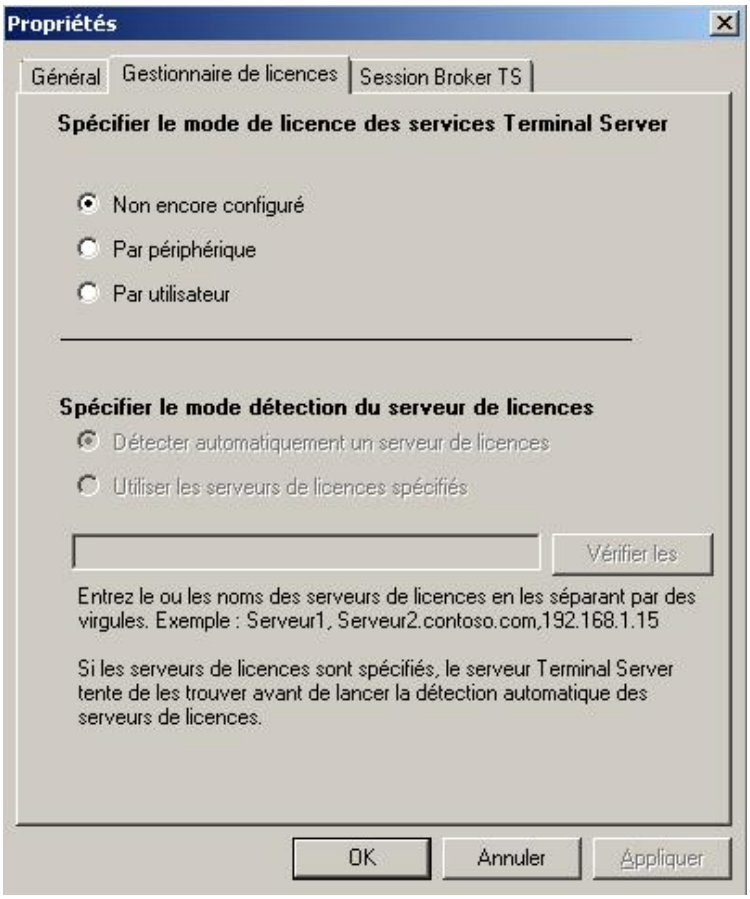
© ENI Editions - All rigths reserved

Sur les serveurs TS, vous devez choisir le mode de licence à appliquer (par périphérique ou par utilisateur). Vous pouvez le faire de façon graphique et individuelle ou par GPO.

Pour spécifier le mode de licence et le nom du serveur de licence de façon graphique :

- Ouvrez la console **Configuration des services Terminal Server** en cliquant sur le bouton **Démarrer**, **Outils d'administration**, puis **Services Terminal Server** et enfin **Configuration des services Terminal Server**.

- Dans le panneau **Configuration du serveur Terminal Server**, double cliquez sur **Mode de licence des services Terminal Server**.


Propriétés
Général
Gestionnaire de licences
Session Broker TS
Spécifier le mode de licence des services Terminal Server
Non encore configuré
Par périphérique
Par utilisateur
Spécifier le mode détection du serveur de licences
Détecter automatiquement un serveur de licences
Utiliser les serveurs de licences spécifiés
Vérifier les
Entrez le ou les noms des serveurs de licences en les séparant par des virgules. Exemple : Serveur1, Serveur2.contoso.com,192.168.1.15
Si les serveurs de licences sont spécifiés, le serveur Terminal Server tente de les trouver avant de lancer la détection automatique des serveurs de licences.
OK
Annuler
Appliquer

Si le service de rôle de gestion des licences TS n'est pas sur un contrôleur de domaine, vous avez la possibilité d'indiquer le ou les noms des serveurs de licences TS.

Pour appliquer le paramétrage via GPO, il faut aller dans : **Configuration ordinateur\Modèle d'administration\Composants Windows\Service Terminal Server\Terminal Server\Gestionnaire de licences**

- Utiliser les serveurs de licences des services Terminal Server indiqués.

- Définir le mode de concession de licences des services Terminal Server.

Vous avez maintenant un serveur de licences TS configuré et fonctionnel.

g. Installer un logiciel sur un serveur TS

Lorsque vous installez un logiciel sur un serveur TSE, vous devez lui indiquer qu'une installation va avoir lieu. Pour se faire, vous pouvez utiliser la commande :

```
change user /install
```

Une fois l'installation terminée, vous pouvez revenir en mode standard :

© ENI Editions - All rigths reserved

```
change user /execute
```

Si l'installeur utilise la technologie MSI, cette commande n'est pas nécessaire, vous pouvez l'exécuter directement.

© ENI Editions - All rigths reserved

Configurations avancées

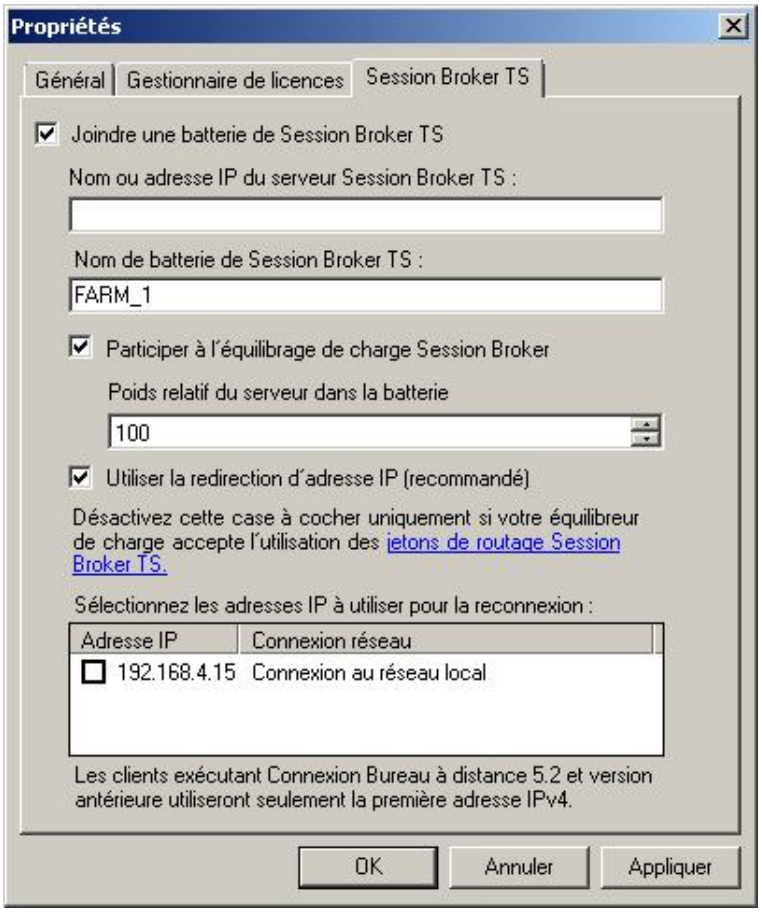
1. Configuration du Session Broker

Ce service de rôle permet de gérer l'ensemble des sessions utilisateurs sur plusieurs serveurs TS. Pour se faire, il stocke l'état de toutes les sessions de tous les serveurs, informations qui lui sont envoyés par les serveurs TS. Quand un utilisateur se connecte pour la première fois sur un serveur, le Session Broker mémorise cette connexion. Si l'utilisateur perd sa connexion réseau, sa session TS reste active sur le serveur, mais en état déconnecté. Quand il aura de nouveau une connexion réseau, et qu'il se connectera de nouveau, le Session Broker détectera qu'il a déjà une session existante, et l'enverra sur ce serveur TS. Ainsi il retrouvera sa précédente session au lieu d'en créer potentiellement une nouvelle.

L'activation du Session Broker peut se faire via 5 GPO, qui se trouve sous : **Configuration ordinateur\Modèle d'administration\Composants Windows\Service Terminal Server\Terminal Server\Session Broker TS**

- **Joindre le service Session Broker TS** : doit être activé pour former une ferme de serveurs TS.
- **Configurez le nom de la batterie de serveurs Session Broker TS** : doit contenir un nom unique par ferme de serveurs à créer.
- **Utiliser la redirection d'adresse IP** : si activée, tout utilisateur ayant déjà une session ouverte sera redirigé sur l'adresse IP du serveur qui possède la session. Le client doit donc pouvoir joindre directement l'adresse IP de chaque serveur TS. Si désactivée, un jeton est fourni au client, qui permet au système d'équilibrage de charge de l'aiguiller sur le bon serveur TS tout en se connectant sur l'adresse IP virtuelle.
- **Configurer le nom du serveur Session Broker TS** : tous les serveurs TS d'une même ferme doivent utiliser le même Session Broker. Il est possible d'indiquer soit le nom netbios, l'adresse IP ou le nom complet (FQDN).
- **Utiliser l'équilibrage de charge de Session Broker TS** : si activée, redirige les nouveaux utilisateurs sur le serveur TS le moins chargé. Si désactivé, le premier serveur contacté sera utilisé.
- La redirection d'adresses IP est obligatoire avec les technologies suivantes de répartition de charges : NLB, à résolution de noms d'hôtes tourniquet (round robin), et tout répartiteur de charge ne prenant pas en charge le jeton de routage Session Broker TS. L'activation peut aussi se faire depuis l'interface graphique : ouvrez la console **Configuration des services Terminal Server** en cliquant sur le bouton **Démarrer**, **Outils d'administration**, puis **Services Terminal Server** et enfin **Configuration des services Terminal Server**.
- Dans le panneau **Configuration du serveur Terminal Server**, double cliquez sur **Membre d'une batterie du serveur Session Broker TS**.

© ENI Editions - All rigths reserved


Propriétés
Général
Gestionnaire de licences
Session Broker TS
Joindre une batterie de Session Broker TS
Nom ou adresse IP du serveur Session Broker TS :
Nom de batterie de Session Broker TS :
FARM_1
Participer à l'équilibrage de charge Session Broker
Poids relatif du serveur dans la batterie
100
Utiliser la redirection d'adresse IP (recommandé)
Désactivez cette case à cocher uniquement si votre équilibreur de charge accepte l'utilisation des jetons de routage Session Broker TS.
Sélectionnez les adresses IP à utiliser pour la reconnexion :
Adresse IP
Connexion réseau
192.168.4.15
Connexion au réseau local
Les clients exécutant Connexion Bureau à distance 5.2 et version antérieure utiliseront seulement la première adresse IPv4.
OK
Annuler
Appliquer

2. Gestion des impressions

La gestion des impressions, et en particulier des pilotes d'imprimantes a toujours été un sujet important en environnement Terminal Service. Windows Server 2008 introduit la fonctionnalité ***Easyprint*** pour palier aux différents problèmes. Elle est implémentée dans tsprint.dll, aussi bien en 32 et 64 bits, tant côté client que serveur. Les pré-requis côté client sont les suivants :

- le client RDC 6.1 (presque tous les rôles de service TS en dépendent) ;
- le Framework .Net 3.0 Service Pack 1.

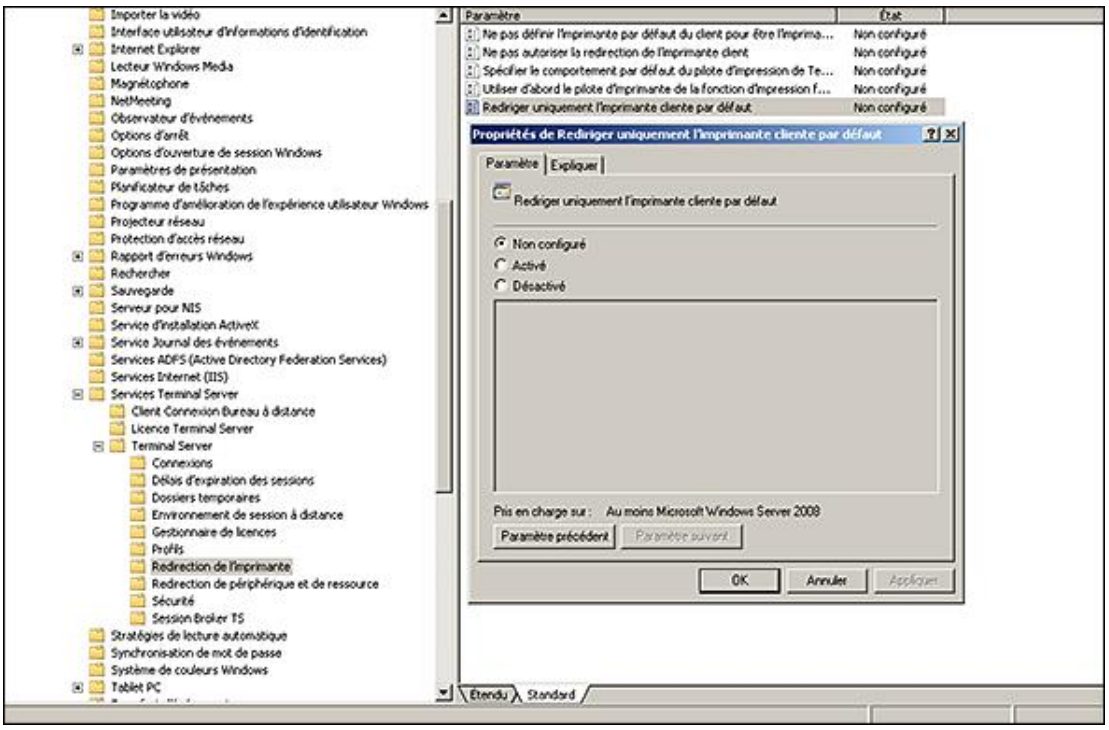
Il est à noter que si le client ne répond pas à ces pré-requis, il faudra installer les pilotes d'imprimantes sur le serveur.

Easyprint permet d'afficher depuis le serveur TS l'ensemble des propriétés de l'imprimante sans avoir à installer le pilote sur le serveur. Pour cela, il se comporte comme un proxy et redirige tous les appels d'interfaces sur le pilote côté client. Il va convertir l'impression du format GDI au format XPS (si le format n'est pas déjà XPS) sur le serveur, et l'envoyer au client dans la session RDP, via un canal virtuel (XPS over RDP). Une fois sur le poste client, si le pilote d'imprimante est compatible XPS, le document est imprimé directement, sinon il est converti de nouveau du format XPS au format GDI et imprimé.

Il est maintenant possible de restreindre le nombre d'imprimantes à connecter depuis le poste client via GPO. L'ouverture de session est accélérée, et l'imprimante par défaut du poste client suffit la plupart du temps.

Pour appliquer cette restriction par GPO, il faut activer le paramètre : **Configuration ordinateur\Modèle d'administration\Composants Windows\Service Terminal Server\Terminal Server\Redirection de l'imprimante**

© ENI Editions - All rigths reserved



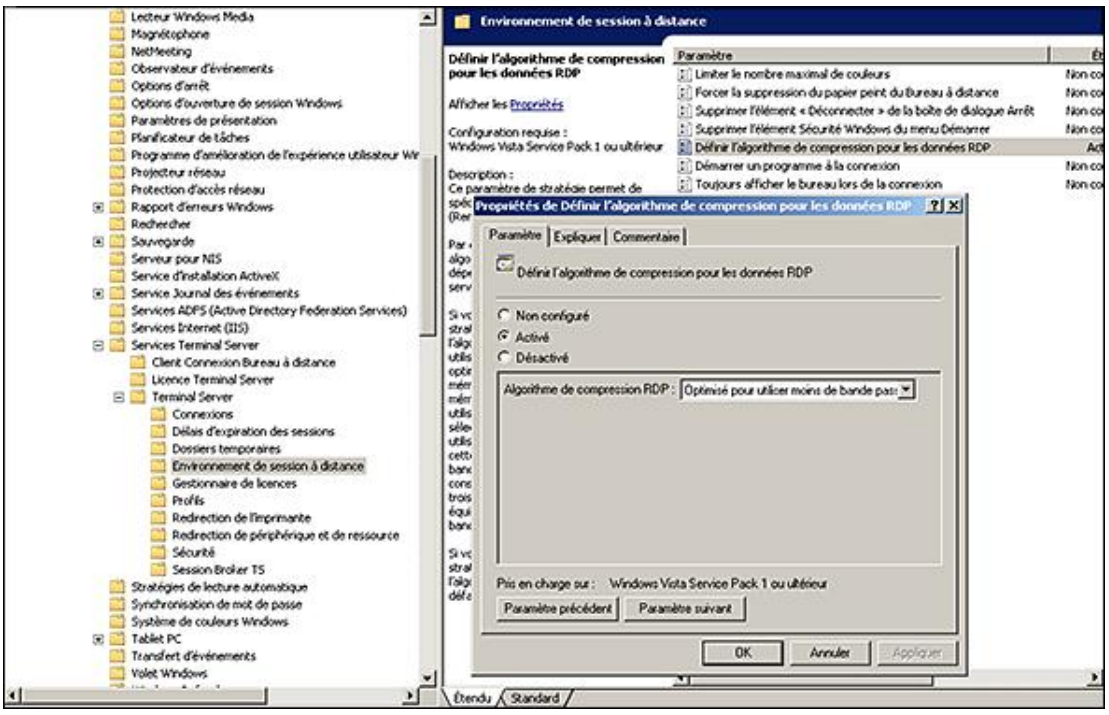
3. Optimiser la bande passante

Des modifications peuvent être apportées afin d'optimiser la consommation réseau générée par les clients :

- Configurer Terminal Services pour utiliser un algorithme de compression plus coûteux.
- Configurer l'affichage pour utiliser du 32 bit, qui consomme moins que le 16 bit (le 24 bit n'existe plus).
- Désactiver l'utilisation de clear type (attention à l'aspect).
- Activer et augmenter le cache RDP persistant sur le client.

Vous pouvez choisir un algorithme plus économique en bande passante et le positionner par stratégie de groupe :

© ENI Editions - All rigths reserved



Les tailles du cache standard et persistant peuvent être configurées en base de registre globalement ou à l'intérieur d'un fichier RDP. Les valeurs sont à positionner sous cette clé : **HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client**

- BitmapCacheSize : a une valeur de 1500 par défaut, avec un maximum de 32000. L'unité de valeur est le Ko. Ce cache est situé en mémoire vive.
- BitmapPersistCacheSize : a une valeur de 10 par défaut. L'unité de valeur est le Ko. Ce cache est situé sur le disque dur.

4. Maintenances

Contrairement à un serveur Web par exemple, passer un serveur Terminal Services en maintenance est plus compliqué vis-à-vis des utilisateurs. Ils peuvent avoir des documents ouverts non sauvegardés, des mails en cours, etc. Heureusement, des outils adaptés sont disponibles, afin de couper le service dans les règles de l'art.

Pour commencer, vous pouvez autoriser ou non les ouvertures de sessions utilisateurs avec la commande `change logon`. Cette commande accepte plusieurs arguments :

- **/QUERY** : affiche le mode d'ouverture de session actuelle.
- **/ENABLE** : autorise les ouvertures de sessions utilisateurs.
- **/DISABLE** : interdit les ouvertures de sessions utilisateurs.
- **/DRAIN** : interdit les nouvelles ouvertures de sessions utilisateurs, mais autorise les reconnexions aux sessions existantes.
- **/DRAINUNTILRESTART** : interdit les nouvelles ouvertures de sessions utilisateurs jusqu'a ce que le serveur ait redémarré, mais autorise les reconnexions aux sessions existantes.

Pour fermer toutes les sessions à la fois, vous pouvez utiliser le script suivant :

```
for /f "skip=2 tokens=2," %i in ('query session') do logoff %i
```

La commande `query session` permet de lister toutes les sessions utilisateurs du serveur.

Une fois la liste des sessions affichée, notez le numéro de session pour lequel vous souhaitez faire une action. Vous

© ENI Editions - All rigths reserved

pouvez ensuite :

- Fermer la session : `logoff XXX`
- Déconnecter l'utilisateur : `tsdicon XXX`
- Supprimer de force une session : `session reset XXX`
- Vous connecter à cette session : `tsconn XXX`
- Envoyer un message à l'utilisateur : `msg XXX « Veuillez fermer votre session »`

© ENI Editions - All rigths reserved

Améliorations avec Windows Server 2008 R2

La seconde édition de Windows Server 2008 amènera des améliorations très notables pour Terminal Services. Vous trouverez ici un aperçu de ces améliorations afin de démontrer, s'il en était besoin, la volonté de Microsoft dans le domaine.

Pour commencer, Microsoft changera le nom du rôle avec Windows Server 2008 R2, Terminal Services devenant « Remote Desktop Services ». Les services de rôles changeront aussi de la façon suivante :

- TS RemoteApp deviendra RemoteApp.
- TS Gateway deviendra RD Gateway.
- TS Session Broker deviendra RD Connection Broker.
- TS Web Access deviendra RemoteApp and Desktop Web Access/ Connections.
- TS Easy Print deviendra RD Easy Print.

Terminal Services et VDI (*Virtual Desktop Infrastructure*) deviendront une solution intégrée. Hyper-V supportera les bureaux virtuels, notamment à travers un broker unique et SCVMM (le gestionnaire de machines Virtuelles).

Un nouveau mécanisme de cache pour les profils utilisateurs évitera de supprimer les profils à la fermeture de session. Un quota sera alloué, et seuls les profils les plus anciens seront automatiquement purgés une fois le quota atteint.

La R2 intégrera aussi le support de PowerShell, un analyseur des meilleurs pratiques, ainsi que le support complet des MSI.

L'expérience utilisateur sera améliorée notamment avec les fonctions suivantes :

- Support du multiécrans étendu à 10 écrans.
- Support de DirectX 10.1 (DXGI 1.1), fonctionnalité Aero Glass.
- Icônes des applications publiées dans le menu démarré, rafraîchit et mis à jour.
- Support d'une barre de langue : configuration des applications avec une langue différente.

Vous savez maintenant mettre en œuvre le rôle Terminal Services avec l'ensemble de ses composants. Vous pouvez mettre en place différentes méthodes d'accès, adaptées à chaque contexte (depuis le réseau local, Internet…) sans réduire la sécurité du système d'information. Il serait dommage de priver ses utilisateurs, donc clients, d'une technologie aussi efficace et rapide.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre sera consacré aux moyens d'accéder aux services de votre société lorsque vous vous trouvez en dehors de celle-ci.

La première partie abordera les différents moyens permettant cet accès distant. Viendront ensuite les différents services offerts par Windows 2008 pour répondre à un besoin de mobilité grandissant.

© ENI Editions - All rigths reserved

Principe de l'accès distant

De nos jours, les utilisateurs nomades sont de plus en plus exigeants et ont besoin d'avoir accès à toutes leurs données en tout temps (mails, fichiers, etc.) de la même façon que s'ils étaient dans les locaux de leur société. Pour pouvoir les satisfaire vous serez certainement amenés à configurer des solutions d'accès distants.

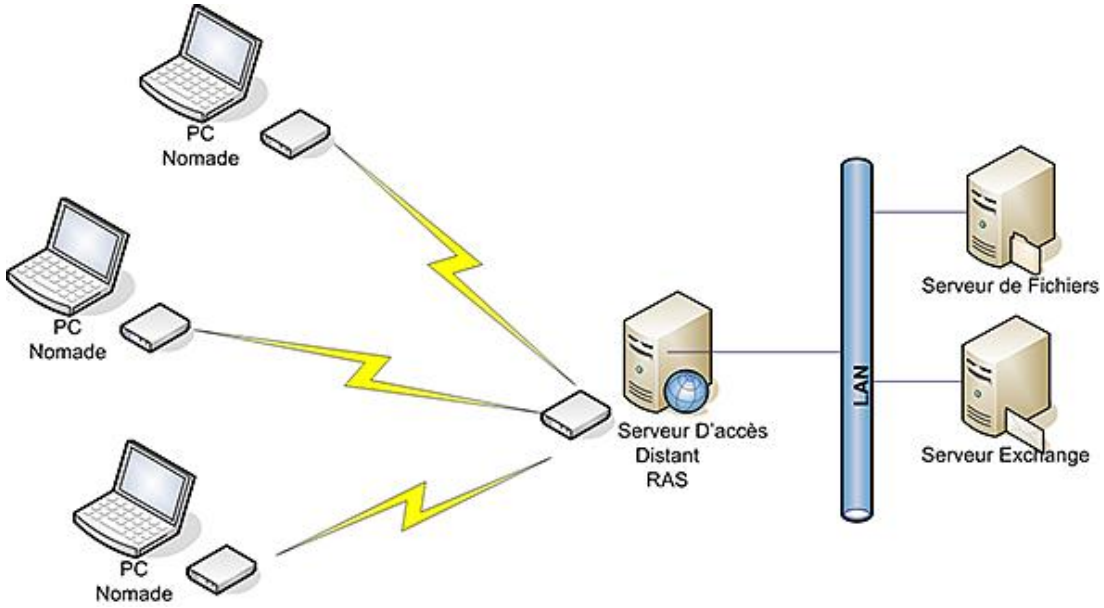
Cet accès distant peut se réaliser au travers de deux types de liaisons. Soit par une liaison de type **Numérotation à la demande** (fréquemment appelée Dial-up), soit par l'établissement d'un **réseau virtuel sécurisé** (VPN : *Virtual Private Network*).

1. Accès par Téléphone

a. Généralités sur les connexions Dial-Up

Utiliser une connexion de type Dial-up permet d'accéder au réseau de l'entreprise au moyen d'une simple ligne téléphonique depuis n'importe quel endroit. Contrepartie de cette facilité d'accès, il s'agit d'une technologie déjà ancienne et qui n'offre que des performances très limitées du fait des bas débits proposés.

En pratique, il faut qu'à la fois le serveur et le PC de l'utilisateur soient munis d'un modem. L'utilisateur configure une connexion de numérotation à la demande dans laquelle un simple numéro de téléphone est spécifié. À l'initiation de la connexion, un nom d'utilisateur et un mot de passe sont requis. Le serveur gérant l'accès distant (appelé aussi RAS pour *Remote Access Server*) va être contacté tout simplement au travers de la ligne téléphonique auquel il est raccordé par le modem.



b. Avantages et inconvénients des connexions Dial-Up

Avantages

- Pas besoin d'abonnement Internet : une simple ligne téléphonique classique suffit.
- Confidentialité des données : les informations ne transitant pas au travers d'Internet, elles ne sont pas cibles de toutes les attaques que l'on trouve communément à travers le réseau de communication mondial. La sécurité est donc maximale car le réseau local n'a pas besoin d'être ouvert sur l'extérieur.

Inconvénients

- Faible bande passante. Basée sur la technologie téléphonique, les débits sont très limités. En effet, le réseau téléphonique a été conçu pour pouvoir reproduire les voix humaines et rien d'autres. Les fréquences pouvant transiter par ce biais devaient donc êtes minimes.

© ENI Editions - All rigths reserved

- Pour augmenter le débit que l'on trouve le plus couramment (56K), il existe des lignes Numeris (128K). Cependant celles-ci représentent un investissement bien plus important.

- Coût élevé. Les communications téléphoniques ont un coût non négligeable, récupérer un simple fichier de 10 Mo devient un investissement en considérant le temps qu'il va falloir mettre pour le télécharger (environ une quarantaine de minutes à une vitesse moyenne de 4ko/s).

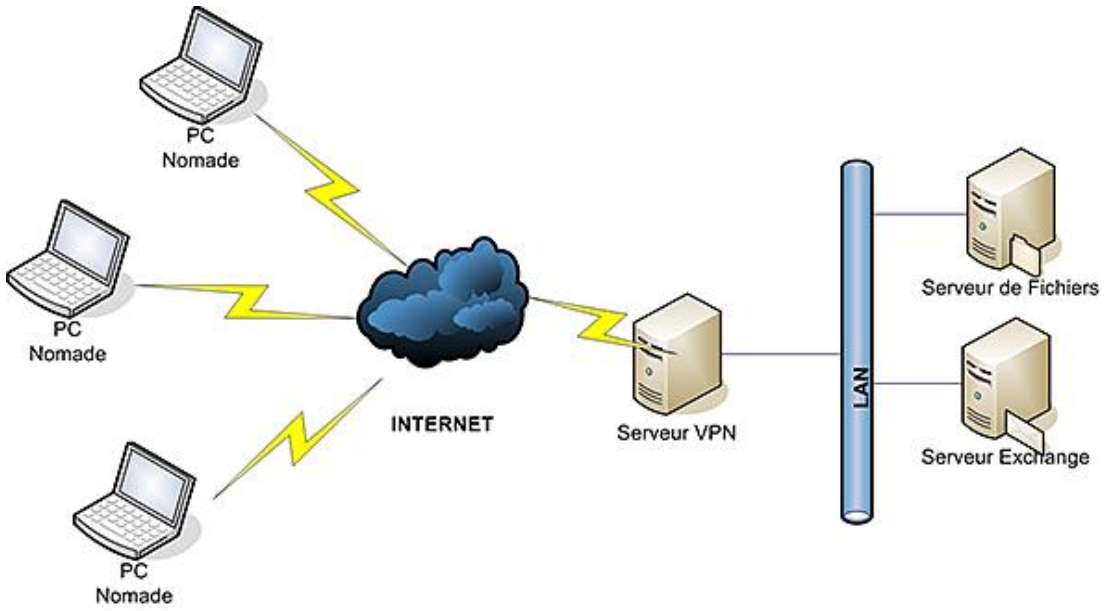
- De plus, fournir des connexions distantes multiples nécessitera autant de lignes téléphoniques que d'utilisateurs nomades pouvant se connecter simultanément.

Bien que le coût très élevé de cette technologie soit un repoussoir notable, elle peut être utilisée dans certains cas très précis. S'il n'est pas rare d'avoir des problèmes de connexion Internet, il est beaucoup plus rare d'avoir des pannes téléphoniques. Il peut être ainsi intéressant de bénéficier de ce type d'accès pour certaines sociétés dans un but d'administration. En effet, un administrateur pourra continuer à gérer des serveurs à distance et ce, même s'ils sont injoignables au travers d'Internet.

2. Accès via Internet

a. Généralités sur les VPN

La seconde technologie permettant l'accès à distance utilise le réseau Internet et non plus le réseau téléphonique. Contrairement aux connexions à la demande qui vous connectent directement au réseau de la société, il est ici nécessaire de passer « au travers » du réseau Internet. La technologie employée est appelée VPN (*Virtual Private Network* ou Réseau Privé Virtuel en français). Ici la communication s'établit directement au niveau IP.

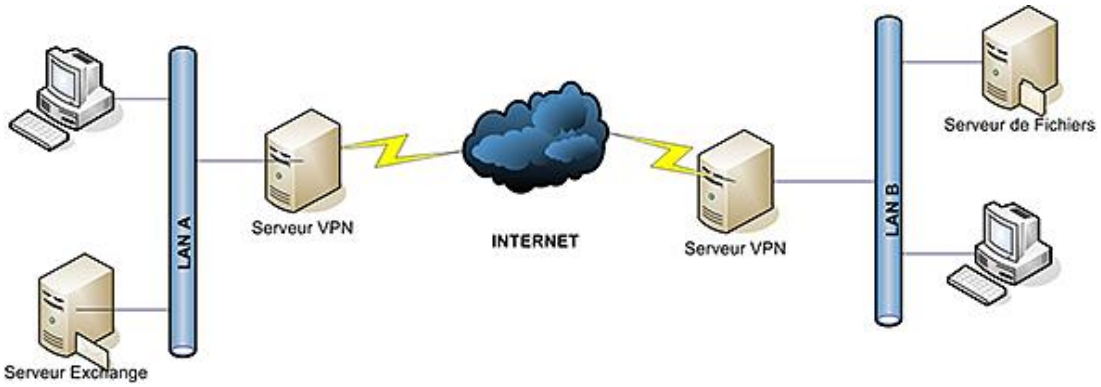


Un peu d'explications concernant la terminologie **Réseau Privé Virtuel** :

La connexion est virtuelle car quand l'ordinateur va établir la connexion VPN à travers Internet, il va agir comme s'il était directement connecté au réseau local, tout comme s'il avait un câble réseau qui y était relié. L'utilisateur va ainsi pouvoir accéder aux mêmes ressources que s'il était physiquement relié au réseau. Cette connexion reste cependant considérée comme virtuelle, justement parce qu'il n'y a pas de liaison Ethernet avec le réseau de destination. Elle est privée car, une connexion point à point entre la source et la destination va être émulée. Les données échangées vont y être chiffrées. De cette façon, si ces données venaient à être interceptées, elles ne pourraient pas être déchiffrées sans la clé privée de la transaction.

Les VPN sont couramment utilisés pour relier des sites distants. On parle alors de VPN site à site. Le but de ce type de connexions est de pouvoir relier logiquement des réseaux distants sans pour autant avoir de liaison réseau directe (Ethernet, Wi-Fi, etc.).

© ENI Editions - All rigths reserved



b. Les différents types de VPN proposés sous Windows Server 2008

Windows Server 2008 comme ses prédécesseurs supporte les types de VPN suivants :

- PPTP (*Point Point Tunneling Protocol*) :

  PPTP est la méthode la plus simple à mettre en œuvre et à utiliser. Le chiffrement des données intervient après le processus d'authentification via le protocole PPP. Préférez une authentification utilisant MSChapv2 à une authentification se basant sur du PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*) afin de ne pas laisser le mot de passe transiter en clair.

- L2TP/IPSec (*Layer 2 Tunneling Protocol*) :

  Plus sécurisé que PPTP, L2TP/IPSec est issu d'un développement conjoint entre Microsoft et Cisco.

  À la différence de PPTP, le chiffrement inclut la phase d'identification puisque la session IPSec est établie juste avant.

  De plus, l'authentification mutuelle des machines (aussi appelée Handshake ou poignée de main en français) empêche toute machine non reconnue de se connecter. Cela évite donc notamment les attaques de type Man-In-Middle dont souffrent les VPN reposant sur du PPTP.

  Attention cependant, il faut théoriquement éviter le NAT avec de l'IPSec car il modifie le contenu des paquets. Cette modification est incompatible avec les mécanismes de protection de l'intégrité des données IPSec. Si des impératifs vous obligent toutefois à utiliser du L2TP sur un réseau "natté", tournez-vous vers la norme NAT-T (NAT Traversal).

Windows Server 2008 apporte aussi une nouveauté :

- SSTP (*Secure Socket Tunneling Protocol*) :

  SSTP est une nouvelle forme de tunnel VPN. Il facilite l'établissement d'une connexion VPN via un pare-feu ou via un périphérique effectuant de la traduction d'adresses réseaux (NAT).

  Cela est rendu possible par l'encapsulation de paquets PPP (*Protocole Point à Point*) dans de l'HTTPS. L'établissement des connexions VPN via un proxy http est aussi rendu possible.

  Disponible avec Windows 2008 et Windows Vista SP1, SSTP utilise des connexions HHTP cryptées avec SSL pour établir des connexions vers les passerelles VPN.

  De la même façon qu'avec L2TP/IPSec, celui-ci ne transmet les informations d'identification qu'une fois la session SSL établie avec la passerelle VPN.

  Aussi appelé PPP/SSL, ce nouveau protocole permet l'utilisation de PPP et EAP pour l'authentification afin de rendre la connexion plus sécurisée encore.

c. Avantages et inconvénients du VPN

Avantages

© ENI Editions - All rigths reserved

- **Coûts réduits** : toutes les sociétés ainsi que les utilisateurs sont généralement déjà équipés d'une connexion Internet. Le coût de l'implémentation est donc minime puisqu'il suffit de rajouter un serveur pour jouer le rôle de serveur VPN. De plus, une seule connexion Internet peut servir à plusieurs connexions distantes simultanées sans devoir faire l'acquisition d'une ligne supplémentaire.

- **Débits élevés** : la technologie VPN s'appuie directement sur l'IP et donc également sur l'infrastructure Internet. Avec la banalisation de l'ADSL et l'explosion des débits associés, cette technologie est donc bien plus rapide que les connexions de type Dial-Up.

- **VPN Anywhere** : petite analogie à la technologie employée sur exchange (RPC over HTTPS) où on encapsule du trafic Outlook au travers de trafic Web sécurisé (HTTPS). Comme expliqué précédemment ici c'est du trafic VPN qui est encapsulé dans de l'HTTPS. La sécurité des réseaux étant souvent une priorité, il est très courant de bloquer tout trafic sortant ne correspondant pas aux besoins de l'entreprise. Il est par contre rare de voir le trafic HTTPS sortant bloqué. De cette façon grâce au SSTP, l'utilisateur doit pouvoir se connecter depuis n'importe quel réseau d'entreprise ou point d'accès Internet.

Inconvénients

- **Dépendant du réseau** : a contrario des connexions à la demande, les performances de l'abonnement Internet de l'un ou l'autre des deux parties (société ou nomade) ont un impact non négligeable sur la qualité des transmissions. Tout problème chez le fournisseur d'accès de l'un ou de l'autre peut provoquer une incapacité totale à communiquer.

- **Confidentialité des données** : bien qu'utilisant des systèmes de chiffrement il n'en reste pas moins que les données transitent au travers d'Internet. Du coup, elles sont potentiellement visibles de tous et ce bien qu'elles soient chiffrées.

© ENI Editions - All rigths reserved

Mettre en place un accès sécurisé à travers Internet

Dans cette partie vous verrez comment configurer votre serveur en tant que serveur d'accès distant. Dans un premier temps, les méthodes pour configurer les différents types de VPN offerts par Windows 2008 (PPTP, L2TP, SSTP) seront décrites. Puis les aspects de sécurisation seront abordés. La configuration d'un serveur RAS avec modem ne sera pas évoquée, la technologie n'étant quasiment plus utilisée.

1. Mise en place d'une liaison VPN

Pré-requis matériel : le serveur doit être muni de deux cartes réseaux. Une connectée à Internet et l'autre connectée au réseau local (LAN). La première se charge d'accepter les connexions VPN entrantes et nécessite une IP fixe (dans notre exemple configurée en 192.168.250.123). La seconde interface réseau fait suivre le trafic entre les connexions VPN et les ressources réseaux du LAN.

Il est techniquement possible dans le cas d'un VPN PPTP ou L2TP de n'avoir qu'une seule carte réseau. Cela sort par contre du cadre des bonnes pratiques Microsoft et les performances peuvent s'en ressentir.

Pré-requis logiciel : pour configurer les VPN **L2TP/IPSec** et **SSTP** vous devez avoir installé un certificat ordinateur sur le serveur.

Un certificat auto-signé peut néanmoins être généré à la fin de la procédure d'installation du service. Attention cependant, ces certificats ne sont pas reconnus par des autorités publiques et vont générer des alertes de sécurité. Ils ne doivent être utilisés qu'à des fins de tests.

Il faut donc leur préférer une autorité de certificat interne (appelé aussi PKI pour *Public Key Infrastructure*) ou mieux encore un certificat signé par une autorité publique. L'avantage d'un certificat signé par une autorité publique est que ce certificat ne nécessite pas le déploiement du certificat de l'autorité de certificats sur les postes clients contrairement à l'utilisation d'un certificat généré par une PKI.

Ci-après un lien vers le TechNet de Microsoft traitant de la mise en place d'une PKI Microsoft : http://technet.microsoft.com/en-us/library/cc872789.aspx

---

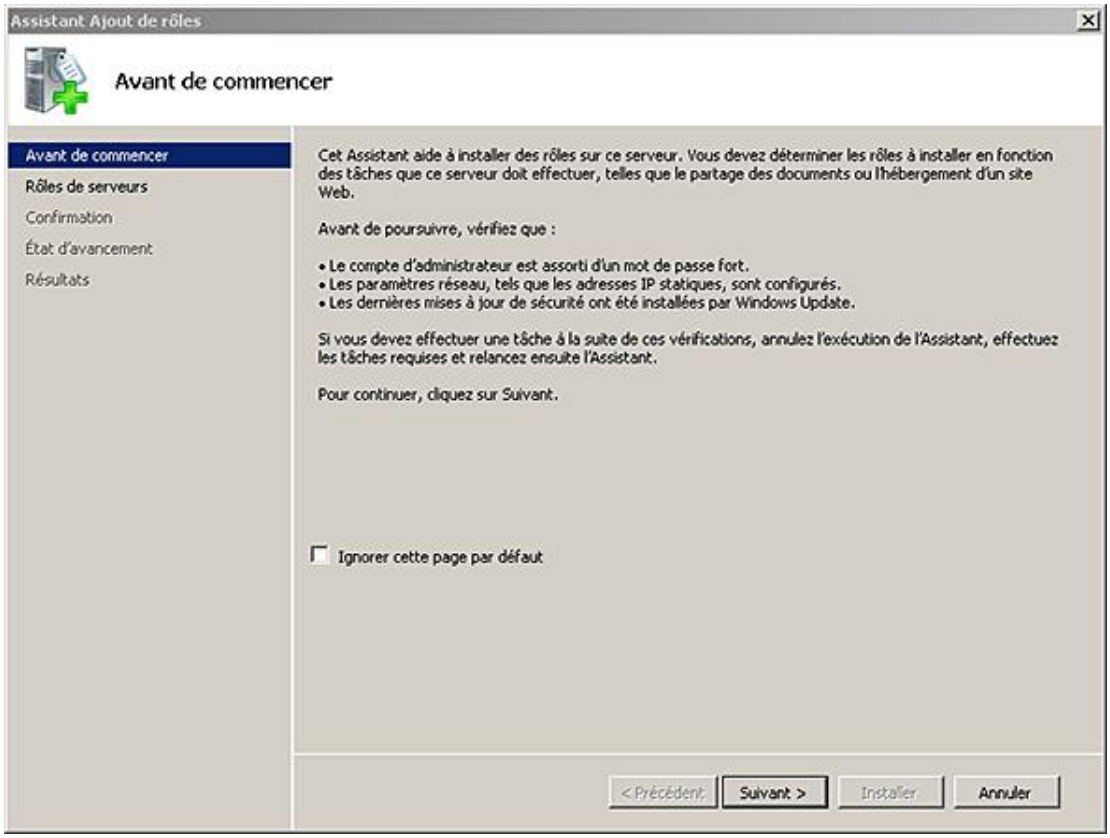
a. Installation du rôle Services de stratégie et d'accès réseau

L'installation du rôle se fait depuis la console **Gestionnaire de Serveur**, dans le sous-dossier **Rôles**, en cliquant sur **Ajouter des rôles**.

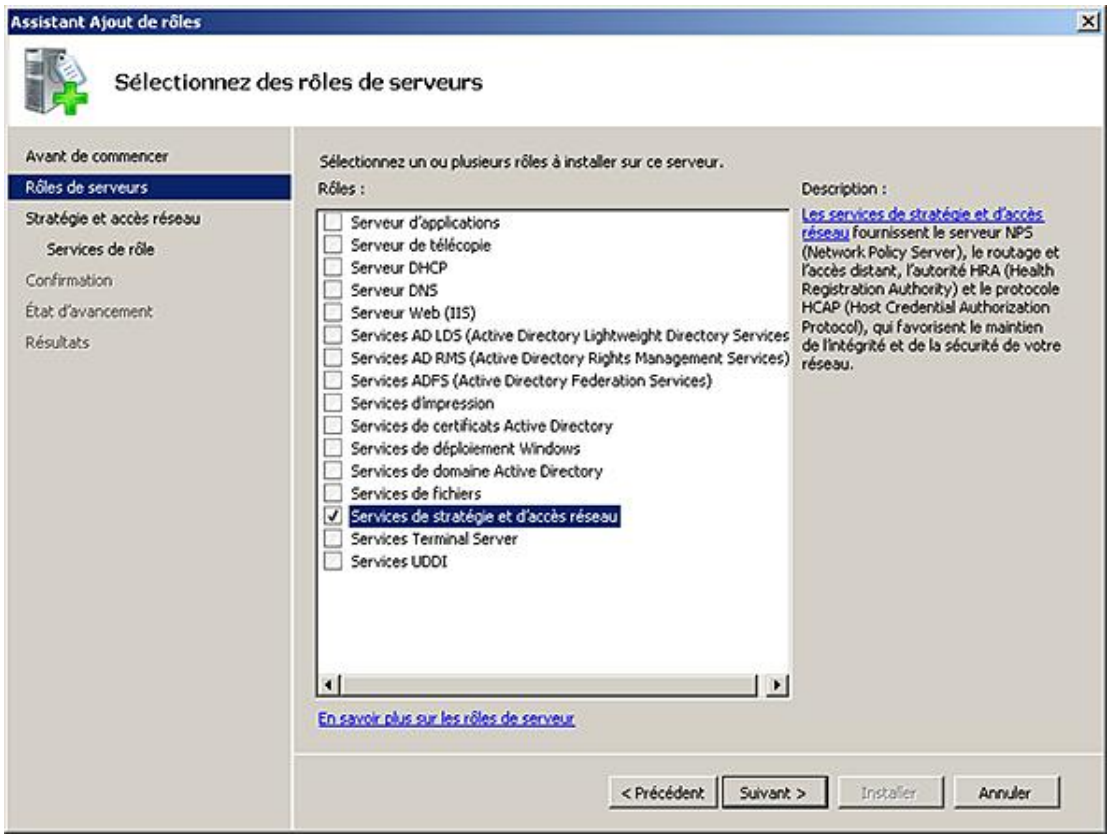
Voici les différentes étapes :

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Gestionnaire de serveur**.

© ENI Editions - All rigths reserved

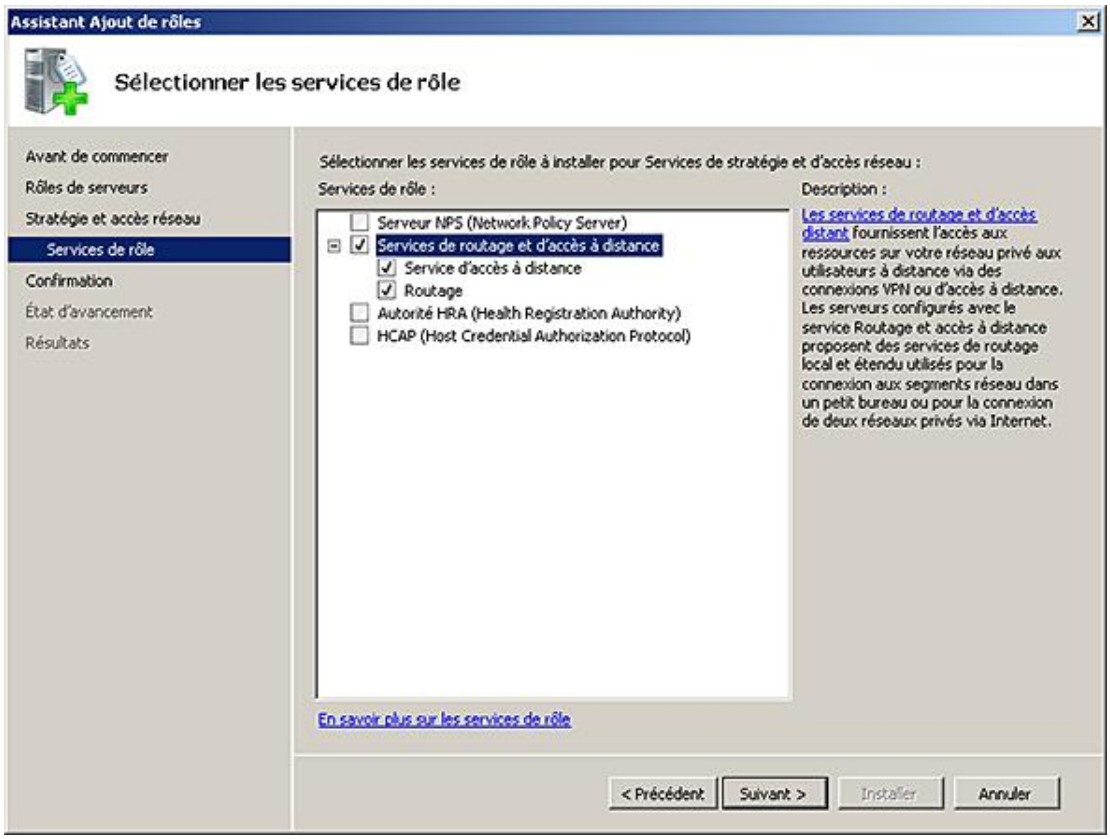

Assistant Ajout de rôles
Avant de commencer
Avant de commencer
Rôles de serveurs
Confirmation
État d'avancement
Résultats
Cet Assistant aide à installer des rôles sur ce serveur. Vous devez déterminer les rôles à installer en fonction des tâches que ce serveur doit effectuer, telles que le partage des documents ou l'hébergement d'un site Web.
Avant de poursuivre, vérifiez que :
• Le compte d'administrateur est assorti d'un mot de passe fort.
• Les paramètres réseau, tels que les adresses IP statiques, sont configurés.
• Les dernières mises à jour de sécurité ont été installées par Windows Update.
Si vous devez effectuer une tâche à la suite de ces vérifications, annulez l'exécution de l'Assistant, effectuez les tâches requises et relancez ensuite l'Assistant.
Pour continuer, cliquez sur Suivant.
Ignorer cette page par défaut
< Précédent
Suivant >
Installer
Annuler

- Cliquez sur **Suivant**.
- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
- Sélectionnez le rôle : **Services de stratégie et d'accès réseau**.


Assistant Ajout de rôles
Sélectionnez des rôles de serveurs
Avant de commencer
Rôles de serveurs
Stratégie et accès réseau
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionnez un ou plusieurs rôles à installer sur ce serveur.
Rôles :
Serveur d'applications
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Services AD LDS (Active Directory Lightweight Directory Services)
Services AD RMS (Active Directory Rights Management Services)
Services ADFS (Active Directory Federation Services)
Services d'impression
Services de certificats Active Directory
Services de déploiement Windows
Services de domaine Active Directory
Services de fichiers
Services de stratégie et d'accès réseau
Services Terminal Server
Services UDDI
Description :
Les services de stratégie et d'accès réseau fournissent le serveur NPS (Network Policy Server), le routage et l'accès distant, l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.
En savoir plus sur les rôles de serveur
< Précédent
Suivant >
Installer
Annuler

© ENI Editions - All rigths reserved

- Sur la page d'**Introduction au service de stratégie et d'accès réseau**, cliquez sur **Suivant**.
- Cochez les cases **Service d'accès à distance** et **Routage** comme illustrée sur l'écran ci-dessous :


Assistant Ajout de rôles
Sélectionner les services de rôle
Avant de commencer
Rôles de serveurs
Stratégie et accès réseau
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Services de stratégie et d'accès réseau :
Services de rôle :
Serveur NPS (Network Policy Server)
Services de routage et d'accès à distance
Service d'accès à distance
Routage
Autorité HRA (Health Registration Authority)
HCAP (Host Credential Authorization Protocol)
Description :
Les services de routage et d'accès distant fournissent l'accès aux ressources sur votre réseau privé aux utilisateurs à distance via des connexions VPN ou d'accès à distance. Les serveurs configurés avec le service Routage et accès à distance proposent des services de routage local et étendu utilisés pour la connexion aux segments réseau dans un petit bureau ou pour la connexion de deux réseaux privés via Internet.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler

- À la page de confirmation, cliquez sur **Installer**.
- Sur la page de **Résultats**, vérifiez que l'installation s'est bien déroulée et cliquez sur **Fermer**.

Pour créer un certificat auto signé pour L2TP/IPSec ou SSTP : ouvrez la console IIS et dans le volet de droite double cliquez sur **Certificats de Serveur**. Dans le panneau d'outils à droite cliquez sur **créez un certificat auto-signé** puis saisissez un nom convivial.

---

b. Configuration des fonctionnalités VPN

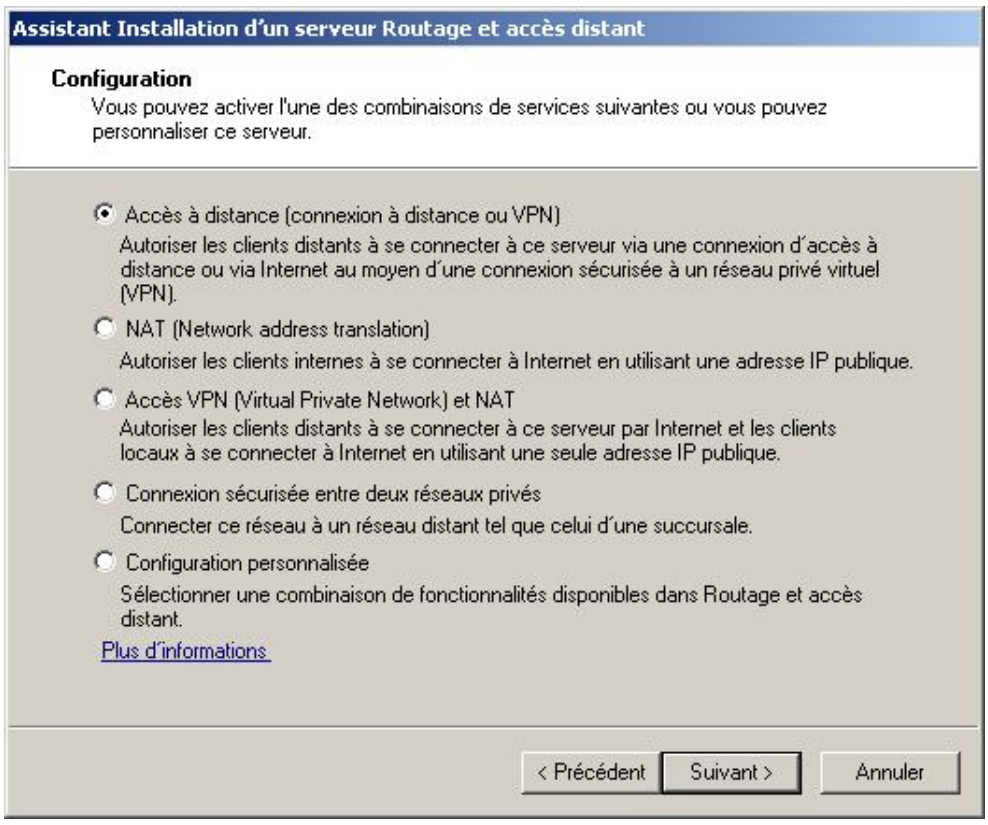
Maintenant que vous avez installé le rôle de serveur d'accès distant, vous allez configurer les paramètres associés.

La procédure de configuration pour les trois technologies VPN est identique. Cependant pour pouvoir utiliser SSTP il faut au préalable avoir satisfait le pré-requis suivant : **Installation du rôle de serveur WEB IIS** abordée dans le chapitre Application Internet - Mettre en place un serveur Intranet/Internet

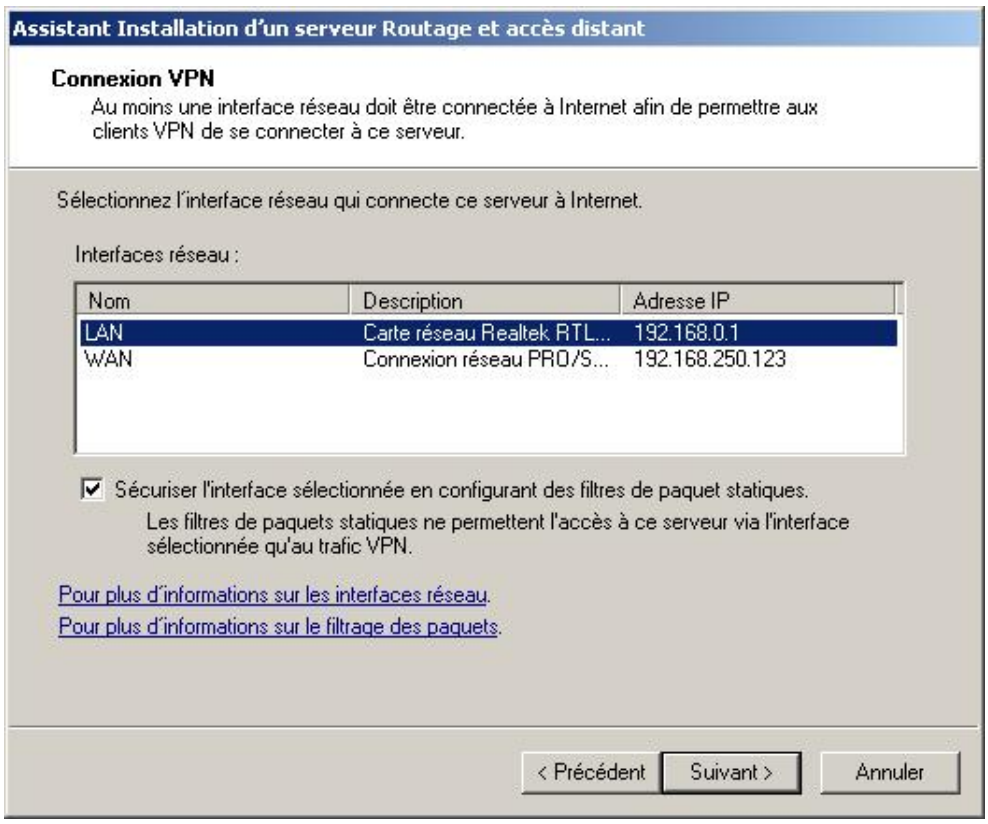
---

- Dans la console **Gestionnaire de Serveur**, développez l'arborescence : **Rôles - Services de stratégie et d'accès réseau**.
- Faites un clic droit sur **Routage et Accès Distant** puis cliquez sur **Configurer et activer le routage et l'accès à distance**.
- L'assistant d'Installation se lance, cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Assistant Installation d'un serveur Routage et accès distant
Configuration
Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.
Accès à distance (connexion à distance ou VPN)
Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).
NAT (Network address translation)
Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.
Accès VPN (Virtual Private Network) et NAT
Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.
Connexion sécurisée entre deux réseaux privés
Connecter ce réseau à un réseau distant tel que celui d'une succursale.
Configuration personnalisée
Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.
Plus d'informations
< Précédent
Suivant >
Annuler

- Sélectionnez **Accès à distance** et cliquez sur **Suivant**.
- Sélectionnez **VPN** et cliquez sur **Suivant**.
- Sélectionnez votre interface publique (ici pour plus de simplicité les connexions ont été renommées en fonction de leur utilisation).


Assistant Installation d'un serveur Routage et accès distant
Connexion VPN
Au moins une interface réseau doit être connectée à Internet afin de permettre aux clients VPN de se connecter à ce serveur.
Sélectionnez l'interface réseau qui connecte ce serveur à Internet.
Interfaces réseau :
Nom
Description
Adresse IP
LAN
Carte réseau Realtek RTL...
192.168.0.1
WAN
Connexion réseau PRO/S...
192.168.250.123
Sécuriser l'interface sélectionnée en configurant des filtres de paquet statiques.
Les filtres de paquets statiques ne permettent l'accès à ce serveur via l'interface sélectionnée qu'au trafic VPN.
Pour plus d'informations sur les interfaces réseau.
Pour plus d'informations sur le filtrage des paquets.
< Précédent
Suivant >
Annuler

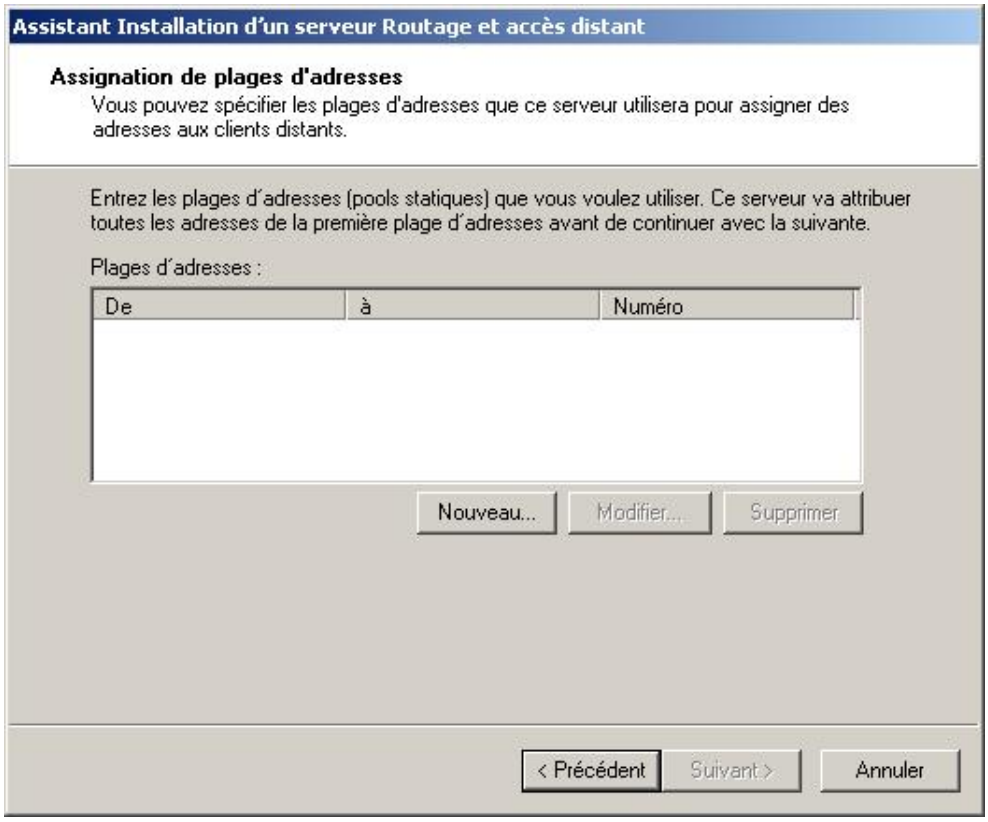
© ENI Editions - All rigths reserved

- Cliquez sur **Suivant**.

- Dans la page **Attribution d'adresses IP**, sélectionnez **Automatiquement** si vous disposez d'un serveur DHCP. Autrement, sélectionnez **A partir d'une plage d'adresses spécifiée**.

- Cliquez sur **Suivant**.

- Si vous choisissez de faire attribuer les adresses par le serveur VPN vous obtiendrez la page suivante.


Assistant Installation d'un serveur Routage et accès distant
Assignation de plages d'adresses
Vous pouvez spécifier les plages d'adresses que ce serveur utilisera pour assigner des adresses aux clients distants.
Entrez les plages d'adresses (pools statiques) que vous voulez utiliser. Ce serveur va attribuer toutes les adresses de la première plage d'adresses avant de continuer avec la suivante.
Plages d'adresses :
De
à
Numéro
Nouveau...
Modifier...
Supprimer
< Précédent
Suivant >
Annuler

- Cliquez sur **Nouveau** puis spécifiez une plage contenant suffisamment d'adresses réseaux. Validez puis cliquez sur **Suivant**.

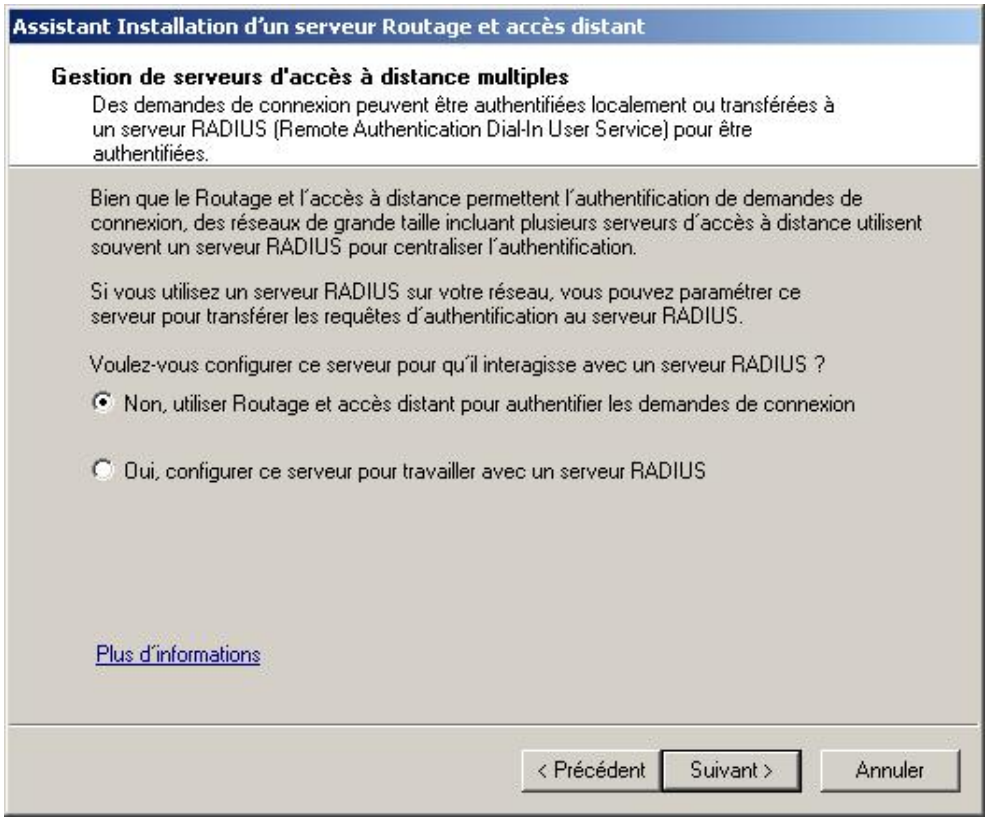
  Attention à bien spécifier une plage correspondant à votre réseau local. Sans cela la communication ne peut pas fonctionner.

Nouvelle plage d'adresse IPv4
Entrez une adresse IP de début et soit une adresse IP de fin, soit le nombre d'adresses contenues dans la plage d'adresses.
Adresse IP de début :
192 . 168 . 0 . 150
Adresse IP de fin :
192 . 168 . 0 . 169
Nombre d'adresses :
20
OK
Annuler

- À la page **Gestion de serveurs d'accès à distance multiples**, si vous disposez d'un serveur RADIUS cochez **Oui**, sinon cochez **Non**.

© ENI Editions - All rigths reserved

Ici vous allez cocher **Non** car la sécurité avec RADIUS est abordée plus tard dans ce chapitre.


Assistant Installation d'un serveur Routage et accès distant
Gestion de serveurs d'accès à distance multiples
Des demandes de connexion peuvent être authentifiées localement ou transférées à un serveur RADIUS (Remote Authentication Dial-In User Service) pour être authentifiées.
Bien que le Routage et l'accès à distance permettent l'authentification de demandes de connexion, des réseaux de grande taille incluant plusieurs serveurs d'accès à distance utilisent souvent un serveur RADIUS pour centraliser l'authentification.
Si vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce serveur pour transférer les requêtes d'authentification au serveur RADIUS.
Voulez-vous configurer ce serveur pour qu'il interagisse avec un serveur RADIUS ?
Non, utiliser Routage et accès distant pour authentifier les demandes de connexion
Oui, configurer ce serveur pour travailler avec un serveur RADIUS
Plus d'informations
< Précédent
Suivant >
Annuler

- Cliquez sur **Suivant**.

- À la page **Résumé**, vérifiez que les informations de configuration sont bien celles désirées puis cliquez sur **Terminer** puis **OK**.

Une fois cet assistant terminé, Windows 2008 crée automatiquement 128 ports pour chacune des trois technologies de VPN qu'il connaît. Chaque connexion requiert un port unique. Pour plus de sécurité il convient d'ailleurs de désactiver les ports inutiles.

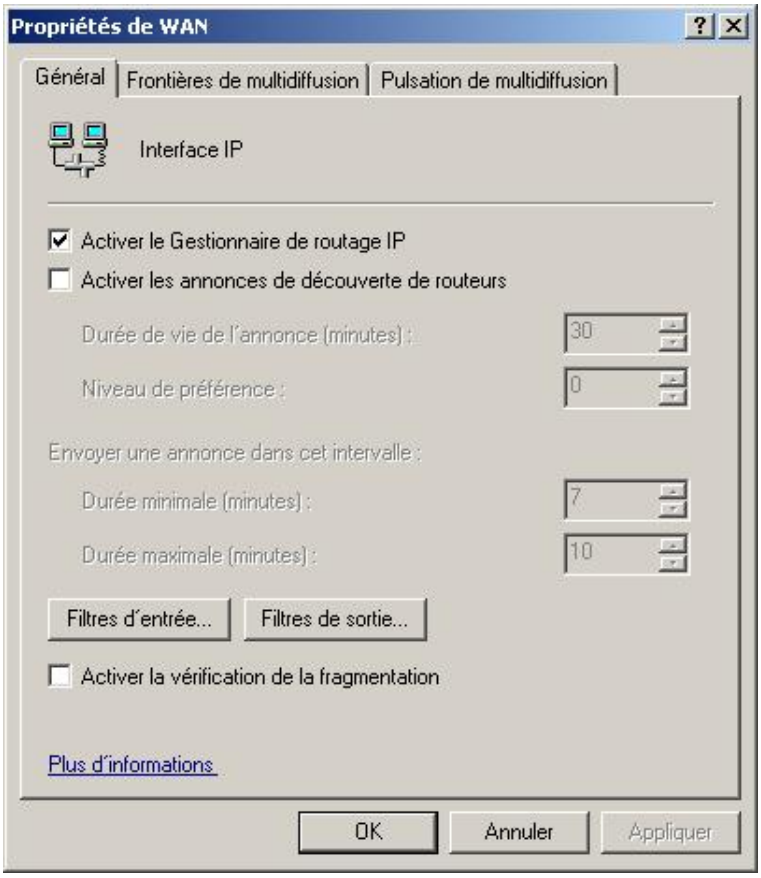
Une fois configuré pour accepter les connexions VPN entrantes, Windows 2008 va automatiquement bloquer tout le trafic entrant sur l'interface publique qui ne correspondrait pas à du trafic VPN.

Pour modifier les paquets autorisés (ex : pour pouvoir prendre la main sur le serveur en bureau distant), il vous faut :

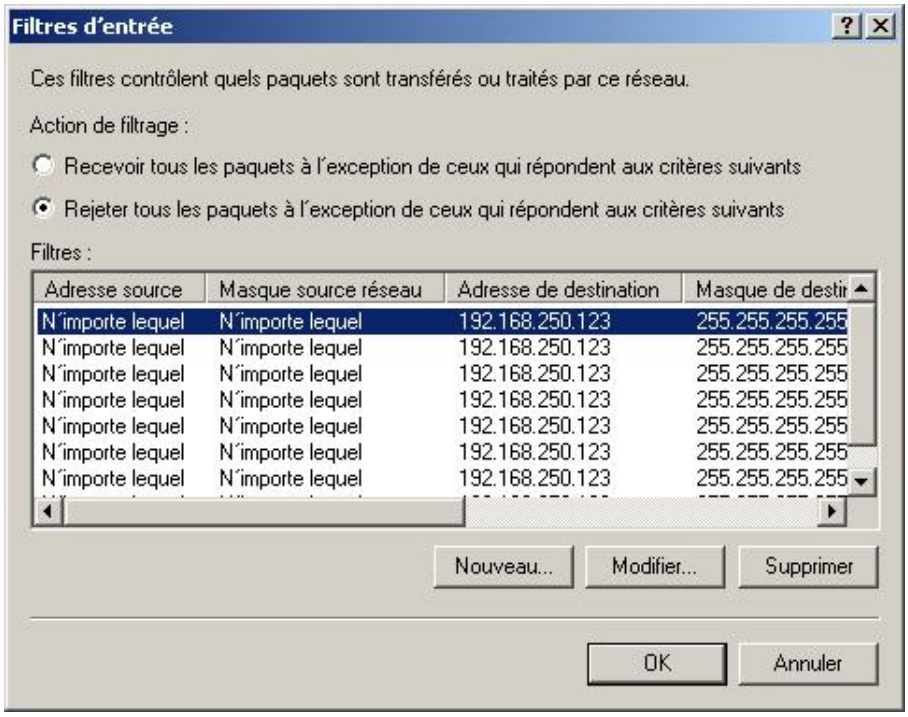
- Depuis la console **Gestionnaire de serveur**, développez **Services de stratégie et d'accès réseau - Routage et accès distant - IPV4** (ou **IPV6** selon votre utilisation) - **Général**.

- Faites un clic droit sur votre interface publique puis sélectionnez **Propriétés**.

© ENI Editions - All rigths reserved



- Cliquez sur **Filtres d'entrée**.



- Il ne vous reste ensuite plus qu'à autoriser le trafic voulu (3389 en TCP par exemple pour le bureau à distance).

2. Gestion de la sécurité des accès

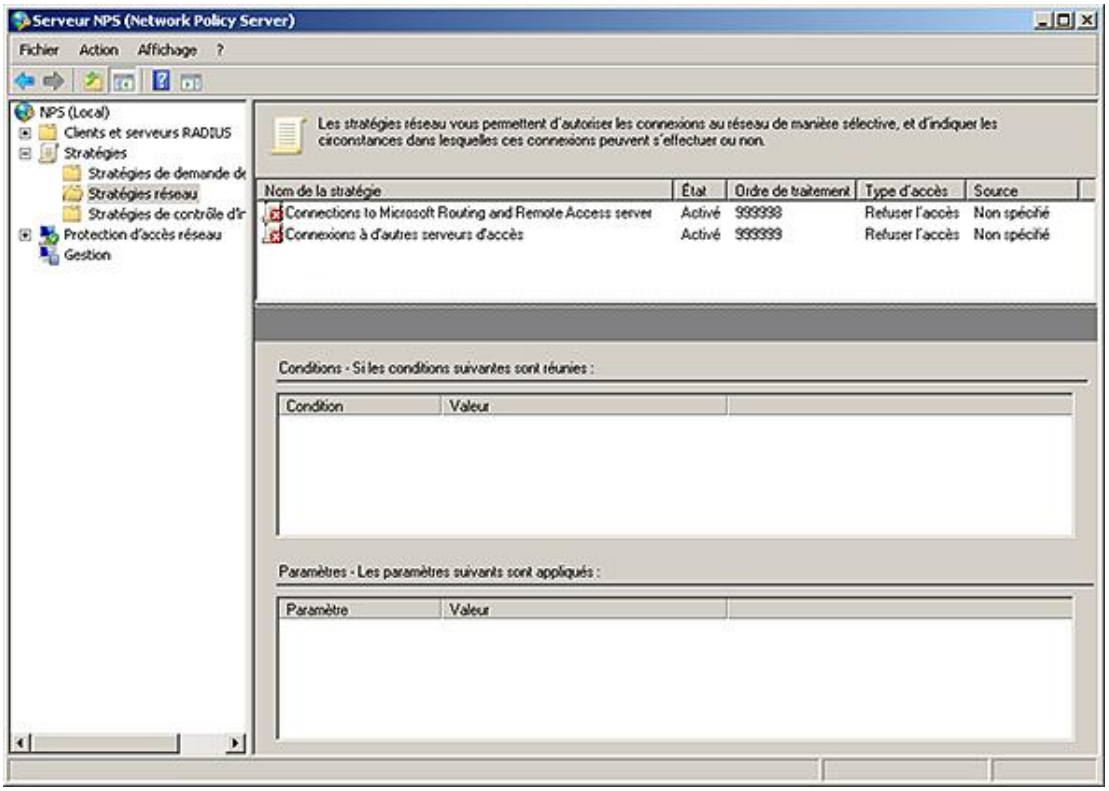
© ENI Editions - All rigths reserved

Maintenant que vous savez configurer votre Windows Server 2008 en tant que serveur d'accès distant, vous voudrez sans doute pouvoir contrôler la manière dont se connectent les utilisateurs. Comptes d'utilisateur, plages horaires, groupes et bien d'autres paramètres encore sont configurables.

Dans les versions précédentes de Windows, ces paramètres étaient configurables via la console stratégies d'accès distant. Désormais vous pourrez utiliser la console **Serveur NPS** (*Network Policy Server*).

Pour modifier une stratégie existante :

- Allez dans **Démarrer - Outils d'administration - Serveur NPS (Network Policy Server)** puis cliquez sur le dossier **Stratégies réseau**



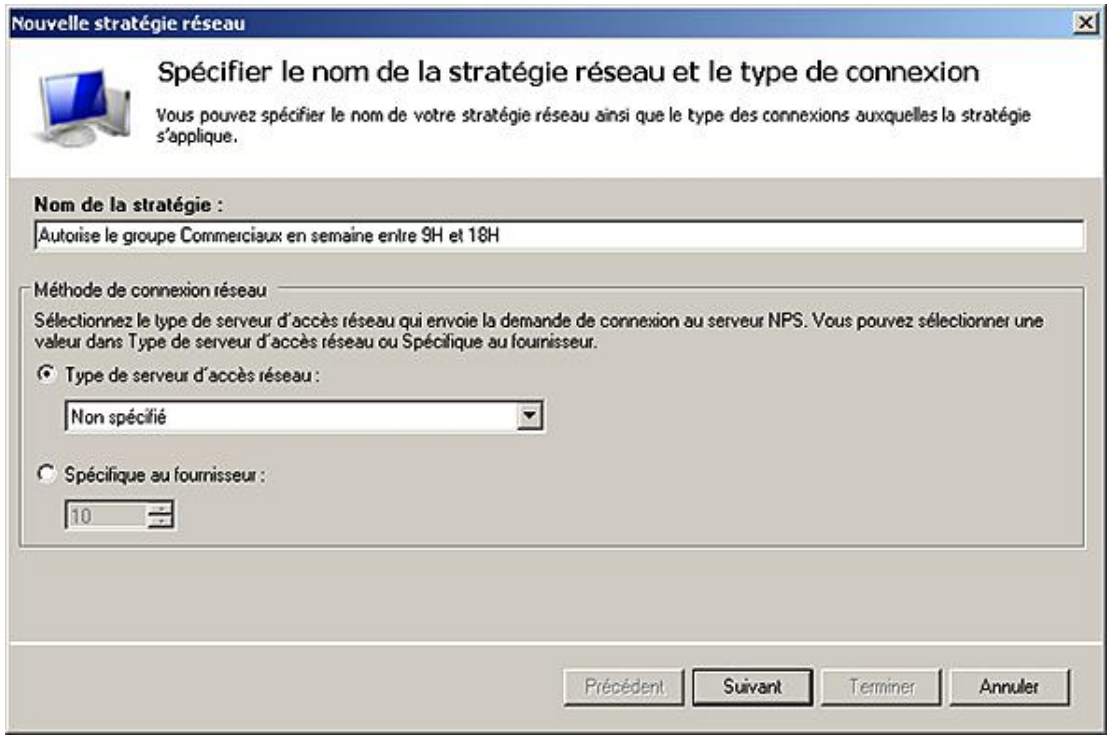
Vous y trouverez deux stratégies par défaut avec des valeurs maximales pour la colonne **Ordre de traitement**. Vous devez faire attention à cet ordre. En effet, les stratégies réseaux sont traitées dans l'ordre croissant. Le serveur va parcourir les stratégies en partant de la plus petite valeur. S'il en trouve une qui correspond aux critères de la demande de connexion, il autorise ou non le trafic. Aussi, si une stratégie est configurée pour refuser l'accès, lors de la vérification des stratégies, l'accès sera automatiquement refusé même si une stratégie venant plus tard l'aurait autorisé.

Le mieux reste de créer vous-même vos stratégies d'accès réseau de façon à maîtriser leur contenu. Voici la marche à suivre pour créer une stratégie autorisant le groupe *Commerciaux* à se connecter en semaine de 9h à 18h :

- Dans la console **Serveur NPS**, allez dans **Stratégies réseaux**.

- Faites un clic droit sur le dossier **Stratégies réseaux** puis cliquez sur **Nouveau**. Spécifiez un nom pour votre stratégie. Attention à mettre des noms explicites, si vos stratégies doivent se multiplier vous gagnerez ainsi en lisibilité.

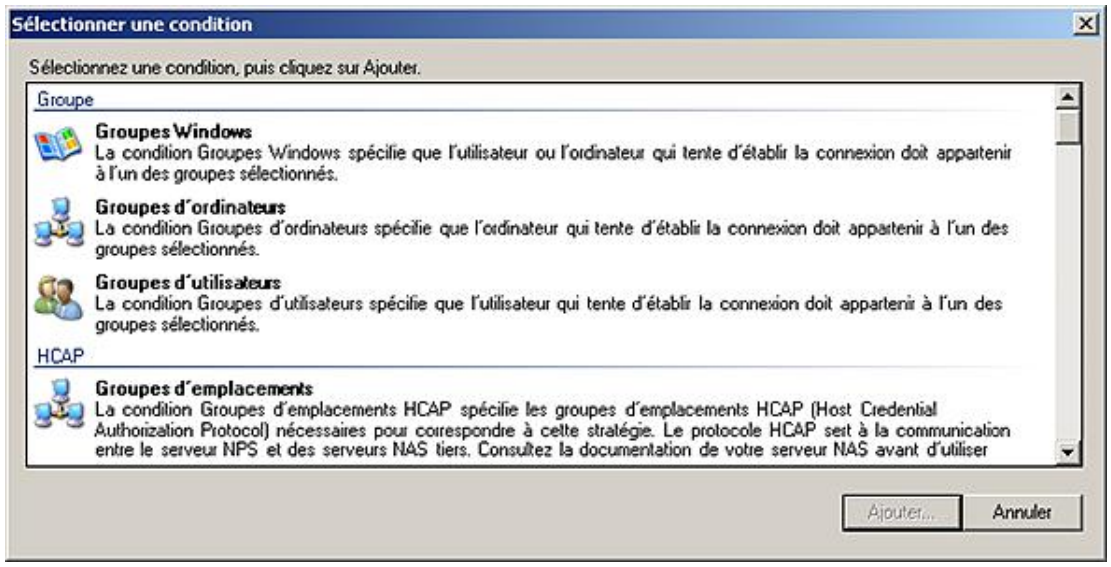
© ENI Editions - All rigths reserved


Nouvelle stratégie réseau
Spécifier le nom de la stratégie réseau et le type de connexion
Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.
Nom de la stratégie :
Autorise le groupe Commerciaux en semaine entre 9H et 18H
Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou Spécifique au fournisseur.
Type de serveur d'accès réseau :
Non spécifié
Spécifique au fournisseur :
10
Précédent
Suivant
Terminer
Annuler

- La liste déroulante **Type de serveur d'accès réseau** réfère à la technologie NAP (*Network Access Protection*) abordée précédemment dans le chapitre Mise en place des services réseaux d'entreprise. Ici ne sera gérée que la sécurité de ce serveur VPN, vous laisserez donc le choix à **Non spécifié**.

- Cliquez sur **Suivant**.

- Vous arrivez ensuite à la page de conditions, cliquez sur **Ajouter**.


Sélectionner une condition
Sélectionnez une condition, puis cliquez sur Ajouter.
Groupe
Groupes Windows
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
Groupes d'ordinateurs
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
Groupes d'utilisateurs
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
HCAP
Groupes d'emplacements
La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser
Ajouter...
Annuler

Vous avez alors la possibilité de choisir parmi une multitude de critères regroupés dans sept groupes distincts :

- Groupe (groupes d'ordinateurs, d'utilisateurs, etc.) ;
- HCAP (groupes correspondant à des serveurs d'accès réseaux tiers) ;
- Restrictions horaires (jours de la semaine, plage horaire, etc.) ;
- Protection d'accès (système d'exploitation, compatibilité NAP, etc.) ;

© ENI Editions - All rigths reserved

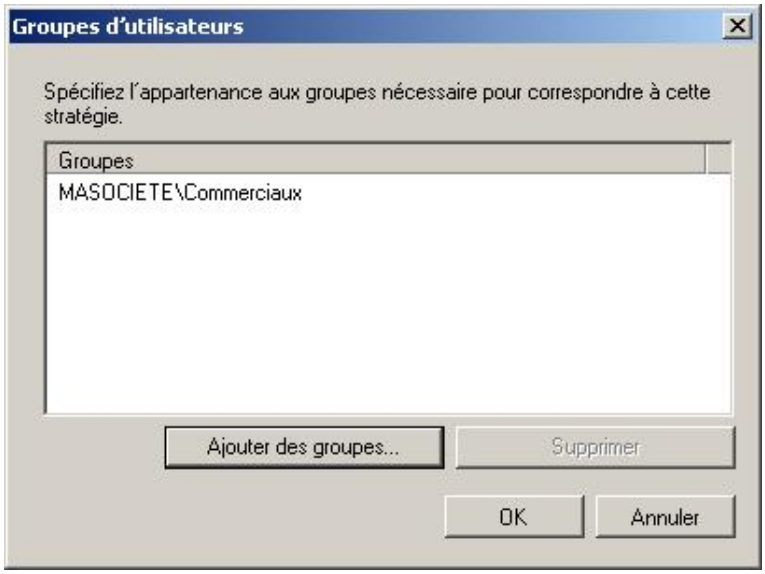
- Propriétés de la connexion (adresse IP du client, type d'authentification, etc.) ;
- Propriétés du client (nom du client RADIUS, IP du client RADIUS, etc.) ;
- Passerelle (numéro de téléphone du serveur Dial-Up, nom du périphérique réseau qui transmet la demande).

La présentation de toutes les conditions ne sera pas faite dans ce livre compte tenu de leur grand nombre. Vous pourrez cependant trouver plus de détails sur le TechNet de Microsoft à l'adresse : http://technet.microsoft.com/en-us/library/cc731220.aspx

---

Les conditions sont cumulables, vous pouvez par exemple faire en sorte d'autoriser l'accès uniquement à un groupe d'utilisateurs et sur une plage horaire bien précise.

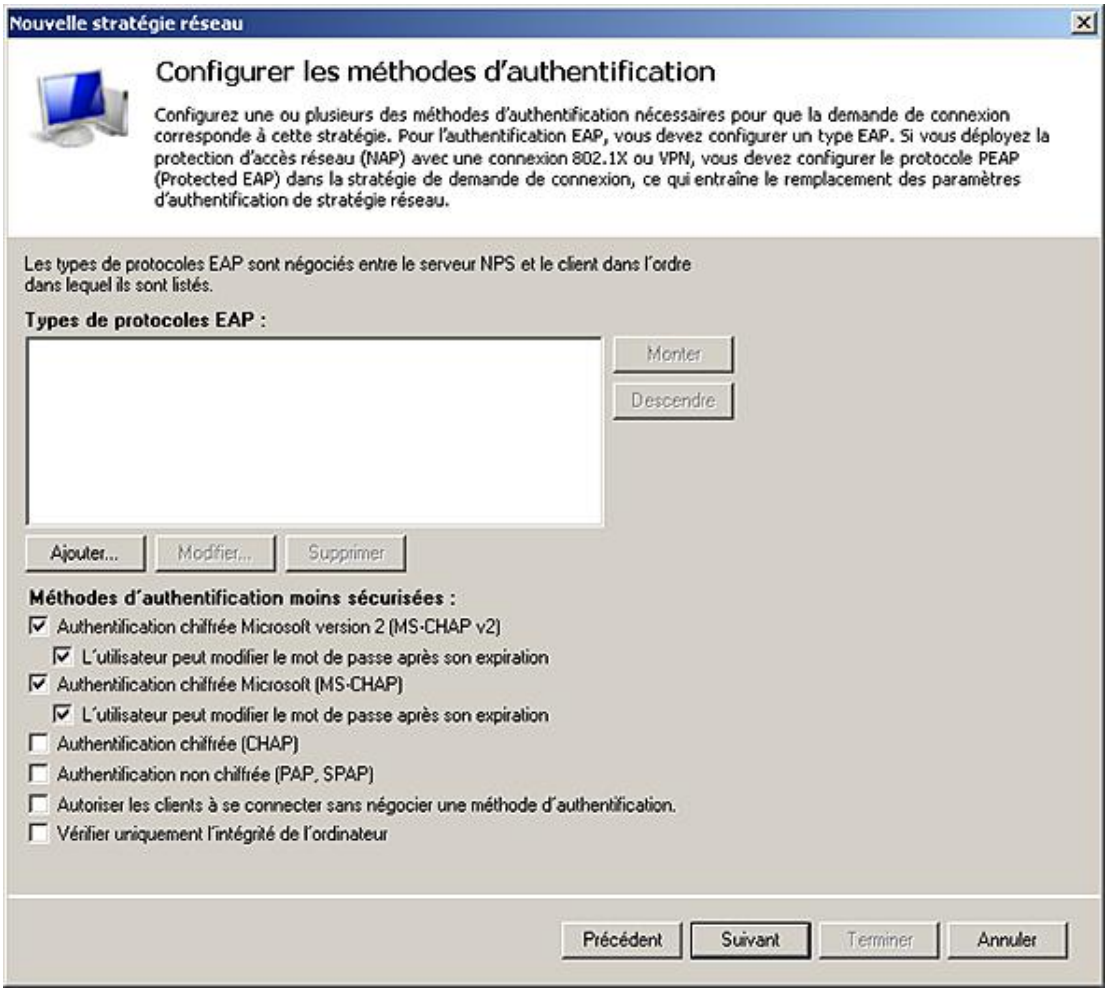
- Sélectionnez **Groupes d'utilisateurs** puis cliquez sur **Ajouter**.
- Dans la boîte de dialogue qui vient d'apparaître cliquez sur **Ajouter des groupes** puis saisissez le nom du groupe (Commerciaux dans notre exemple) puis validez par **OK**.



- Validez par **OK** puis cliquez sur **Suivant**.
- Une fois vos conditions ajoutées, vous avez le choix **D'accorder l'accès**, de **Refuser l'accès** ou encore de faire en sorte que ce soient les **propriétés de numérotation des utilisateurs qui déterminent l'accès** (dans ce cas ce sont les propriétés définies dans le compte de l'utilisateur qui sont prises en compte). Dans cet exemple, choisissez **D'accorder l'accès** puis cliquez sur **Suivant**.
- Vous avez ensuite le choix entre les différentes **Méthodes d'authentification**.

  Vous devez en choisir au moins une. Attention cependant, les cases non cochées dans l'image ci-dessous représentent des authentifications peu sécurisées et ne sont donc pas à cocher dans la mesure du possible.
- Ici laissez les cases cochées par défaut.

© ENI Editions - All rigths reserved

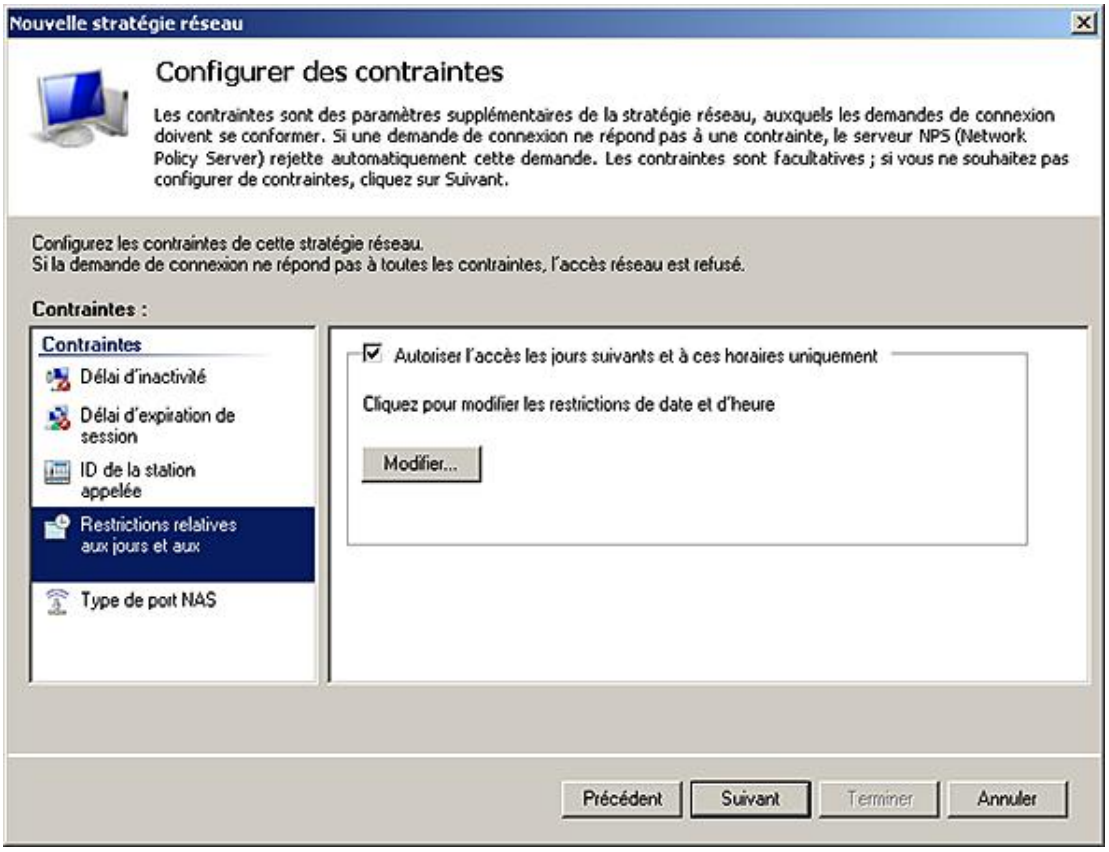

Nouvelle stratégie réseau
Configurer les méthodes d'authentification
Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP. Si vous déployez la protection d'accès réseau (NAP) avec une connexion 802.1X ou VPN, vous devez configurer le protocole PEAP (Protected EAP) dans la stratégie de demande de connexion, ce qui entraîne le remplacement des paramètres d'authentification de stratégie réseau.
Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.
Types de protocoles EAP :
Monter
Descendre
Ajouter...
Modifier...
Supprimer
Méthodes d'authentification moins sécurisées :
Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée Microsoft (MS-CHAP)
L'utilisateur peut modifier le mot de passe après son expiration
Authentification chiffrée (CHAP)
Authentification non chiffrée (PAP, SPAP)
Autoriser les clients à se connecter sans négocier une méthode d'authentification.
Vérifier uniquement l'intégrité de l'ordinateur
Précédent
Suivant
Terminer
Annuler

- Cliquez sur **Suivant**.

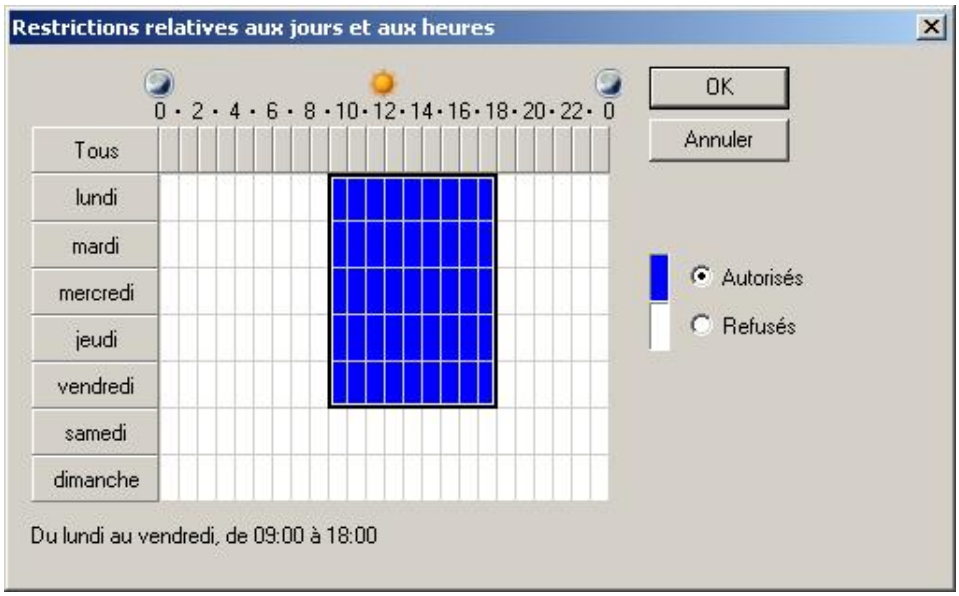
La page de contraintes permet d'appliquer des restrictions supplémentaires comme la plage horaire autorisée (cas de notre exemple).

- Cliquez sur **Restrictions relatives aux jours et aux** puis cochez la case **Autoriser l'accès les jours suivants et à ces horaires uniquement**.

© ENI Editions - All rigths reserved


Nouvelle stratégie réseau
Configurer des contraintes
Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.
Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes :
Contraintes
Délai d'inactivité
Délai d'expiration de session
ID de la station appelée
Restrictions relatives aux jours et aux
Type de port NAS
Autoriser l'accès les jours suivants et à ces horaires uniquement
Cliquez pour modifier les restrictions de date et d'heure
Modifier...
Précédent
Suivant
Terminer
Annuler

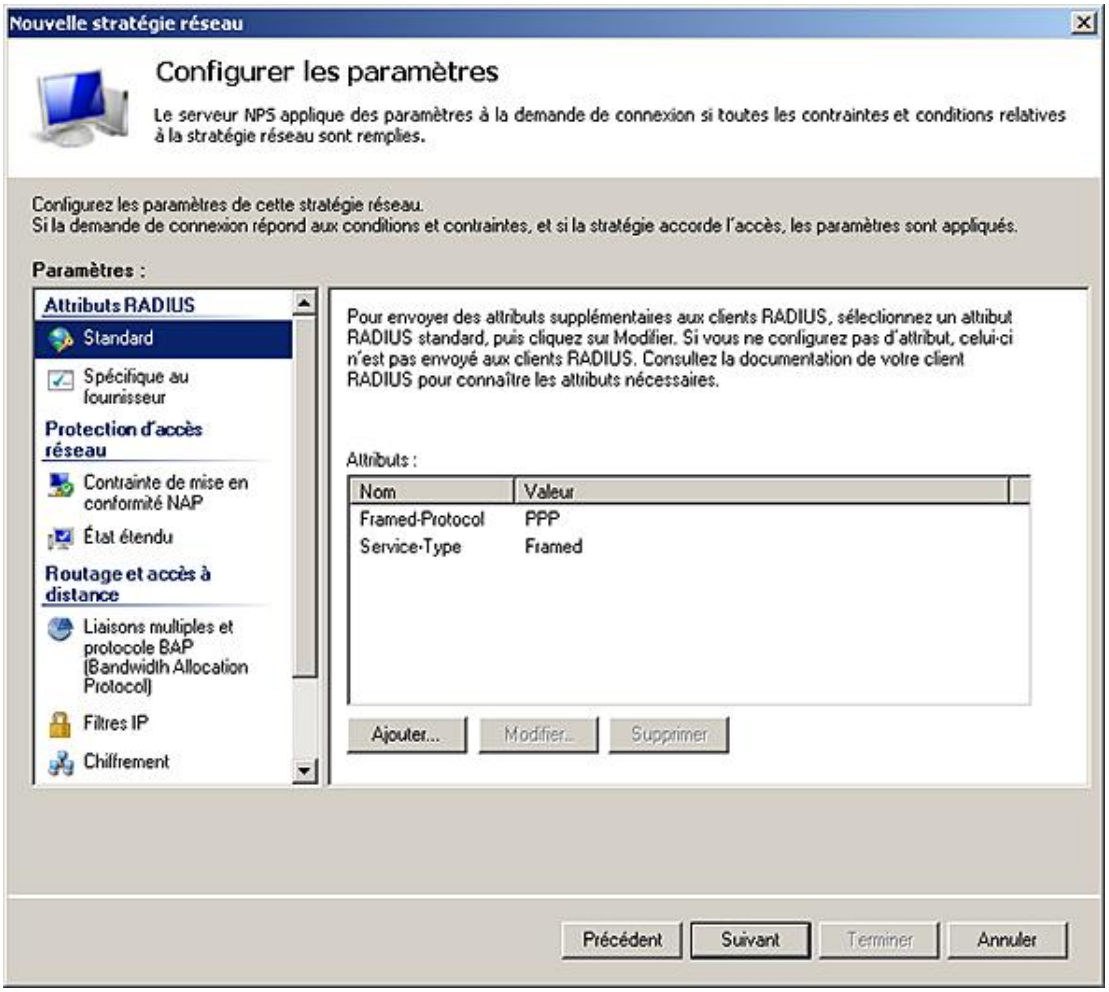
- Cliquez sur **Modifier** puis remplissez comme ci-après pour autoriser les jours de semaine entre 9h et 18h.



- Validez en cliquant **OK** puis cliquez sur **Suivant**.

- Dans cette fenêtre vous pouvez configurer des paramètres supplémentaires pour sécuriser la connexion. En effet, si la connexion répond aux critères précédents, à savoir conditions et contraintes, elle se voit appliquer des paramètres supplémentaires. Cela va de la mise en conformité via NAP à un chiffrement de la connexion ou encore à une restriction sur les protocoles utilisés pendant la connexion. Pour cet exemple, ne spécifiez pas de paramètres et cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Nouvelle stratégie réseau
Configurer les paramètres
Le serveur NPS applique des paramètres à la demande de connexion si toutes les contraintes et conditions relatives à la stratégie réseau sont remplies.
Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.
Paramètres :
Attributs RADIUS
Standard
Spécifique au fournisseur
Protection d'accès réseau
Contrainte de mise en conformité NAP
État étendu
Routage et accès à distance
Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
Filtres IP
Chiffrement
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Framed-Protocol
PPP
Service-Type
Framed
Ajouter...
Modifier...
Supprimer
Précédent
Suivant
Terminer
Annuler

- Sur la dernière page de l'assistant, vérifiez bien les informations saisies puis cliquez sur **Terminer**.

- Votre nouvelle stratégie apparaît avec un chiffre appliqué automatiquement pour l'ordre de traitement. Vous pouvez ensuite, à loisir, modifier cet ordre en faisant un clic droit sur la stratégie. Puis en choisissant une des options **Monter** ou **Descendre**. Cela vous permet de définir sa priorité et donc l'ordre dans lequel elle est vérifiée lors d'une demande de connexion.

3. Gestion de l'authentification (IAS/Radius)

Dans la partie précédente vous avez vu comment configurer une stratégie de connexion pour l'accès via VPN grâce à la console NPS. Bien que techniquement faisable, cela devient rapidement ingérable de le faire lorsque vous disposez de plusieurs serveurs d'accès réseaux (serveurs VPN, bornes Wi-Fi, etc.).

Pour centraliser la gestion des règles d'accès et de l'authentification vous avez besoin du composant de service **NPS** (*Network Policy Server*). Ce rôle était connu dans les versions précédentes de Windows Server sous le nom d'IAS (*Internet Authentication Service*).

Pour centraliser l'authentification, utilisez le rôle de **serveur RADIUS**. L'intérêt de la technologie RADIUS est de pouvoir centraliser la gestion de la sécurité d'équipements informatiques autres que Microsoft. En effet, vous pouvez par exemple configurer un point d'accès Wi-Fi pour utiliser le serveur NPS Windows Server 2008 pour gérer l'authentification.

Voici les fonctions que vous offre le rôle de Serveur NPS en matière de sécurisation :

- **Network Policy Server (NPS)** : authentification, autorisation, services pour serveurs d'accès distants, VPN, points d'accès Wi-Fi, Passerelle TS.

- **NPS Accounting (ou journalisation)** : audit et enregistrement des authentifications et des requêtes de compte dans une base SQL ou un fichier local.

© ENI Editions - All rigths reserved

- **NPS Radius Proxy** : permet l'acheminement des messages entre les clients RADIUS (serveurs d'accès et les serveurs RADIUS qui s'occupent de l'authentification).
- **NPS NAP** : reportez-vous au chapitre Mise en place des services réseaux d'entreprise - Quarantaine réseau.
- **NPS Radius serveur** : gère l'authentification, l'autorisation et l'enregistrement des demandes des clients RADIUS.
- **NPS Radius Client** : serveur d'accès distant utilisant un serveur RADIUS pour l'authentification.

Les ordinateurs clients ne sont pas des clients RADIUS. Ce sont les équipements auxquels ils se connectent (serveur VPN, point d'accès Wi-Fi) qui le sont.

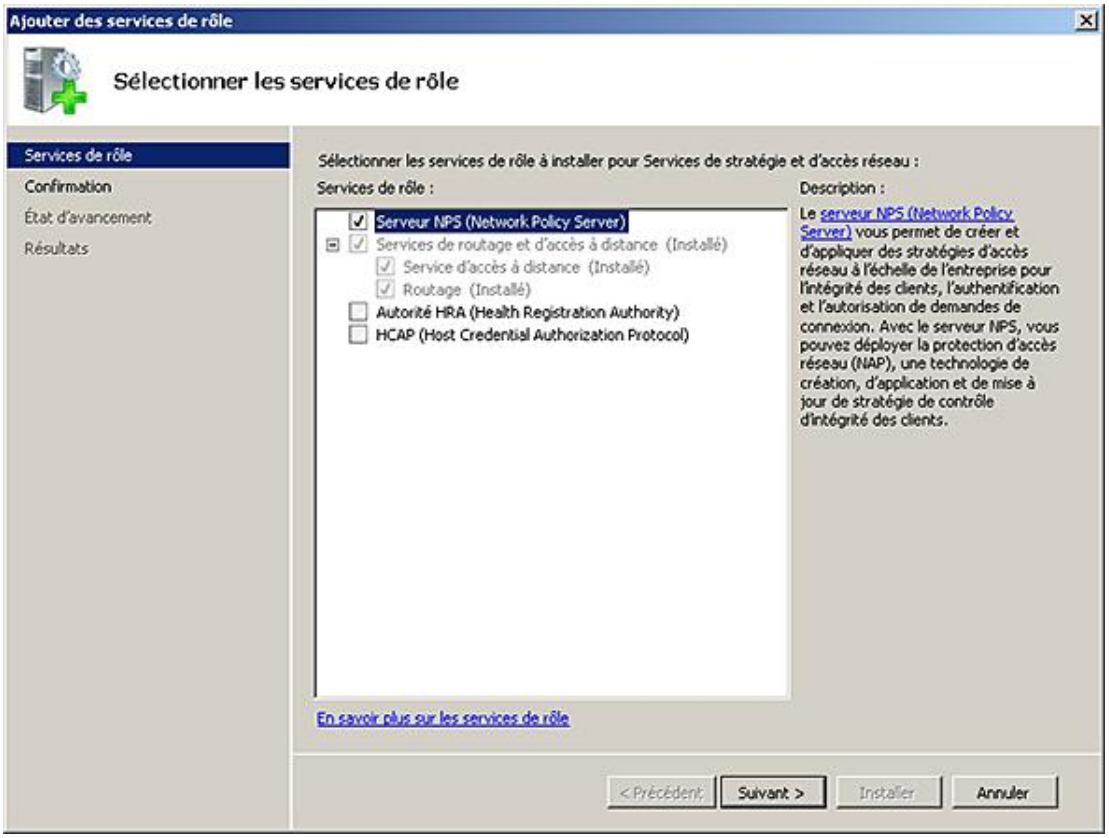
Dans les rubriques précédentes de ce chapitre vous avez vu comment ajouter le rôle de serveur d'accès distant. Pour pouvoir installer le composant NPS, procédez comme suit :

- Dans la console **Gestionnaire de Serveur**, naviguez jusqu'à : **Rôles - Services de stratégies d'accès distant**.
- Dans la fenêtre de droite, cliquez sur **Ajouter des services de rôle**.

Gestionnaire de serveur
Fichier Action Affichage ?
Gestionnaire de serveur (MASOCIE
Rôles
Services de stratégie et d'a
Routage et accès distar
Fonctionnalités
Diagnostics
Configuration
Stockage
Services de stratégie et d'accès réseau
Fournit la prise en charge pour le routage réseau, les réseaux privés virtuels et les stratégies d'accès réseau.
Services de rôle : 3 installé(s)
Ajouter des services de rôle
Supprimer des services de rôle
Service de rôle
État
Serveur NPS (Network Policy Server)
Non installé(s)
Services de routage et d'accès à distance
Installé
Service d'accès à distance
Installé
Routage
Installé
Autorité HRA (Health Registration Authority)
Non installé(s)
HCAP (Host Credential Authorization Protocol)
Non installé(s)
Description :
Le serveur NPS (Network Policy Server) vous permet de créer et d'appliquer des stratégies d'accès réseau à l'échelle de l'entreprise pour l'intégrité des clients, l'authentification et l'autorisation de demandes de connexion. Avec le serveur NPS, vous pouvez déployer la protection d'accès réseau (NAP), une technologie de création, d'application et de mise à jour de stratégie de contrôle d'intégrité des clients.
Dernière actualisation : 02/01/2009 11:42:38
Configurer l'actualisation

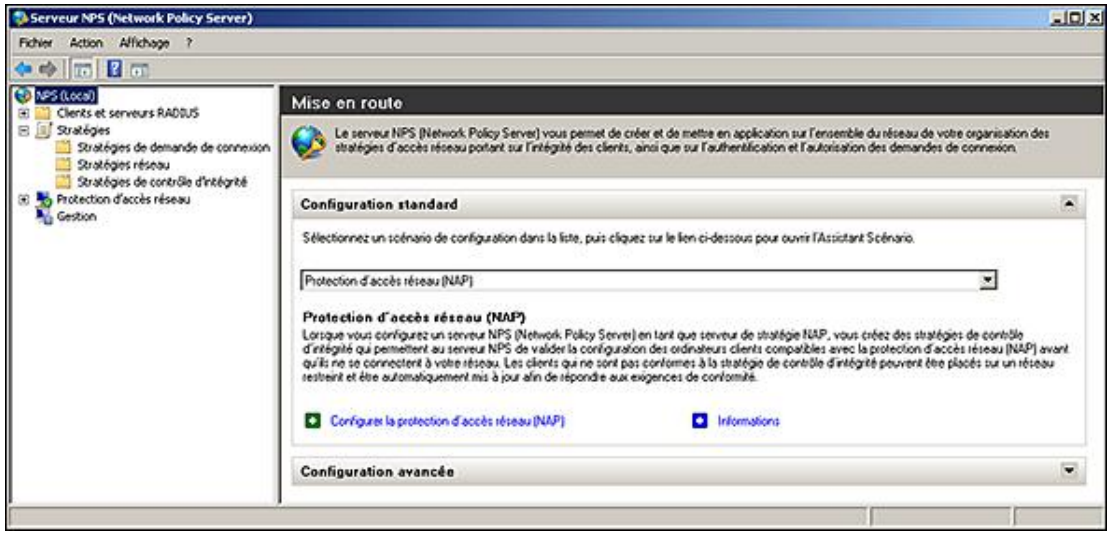
- Cochez la case **Serveur NPS (Network Policy Server)** comme figuré dans l'image ci-après puis cliquez sur **Suivant**.
- Cliquez ensuite sur **Installer**.

© ENI Editions - All rigths reserved


Ajouter des services de rôle
Sélectionner les services de rôle
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Services de stratégie et d'accès réseau :
Services de rôle :
Serveur NPS (Network Policy Server)
Services de routage et d'accès à distance (Installé)
Service d'accès à distance (Installé)
Routage (Installé)
Autorité HRA (Health Registration Authority)
HCAP (Host Credential Authorization Protocol)
Description :
Le serveur NPS (Network Policy Server) vous permet de créer et d'appliquer des stratégies d'accès réseau à l'échelle de l'entreprise pour l'intégrité des clients, l'authentification et l'autorisation de demandes de connexion. Avec le serveur NPS, vous pouvez déployer la protection d'accès réseau (NAP), une technologie de création, d'application et de mise à jour de stratégie de contrôle d'intégrité des clients.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler

- Une fois l'installation terminée, cliquez sur **Fermer**.

Vous pouvez désormais gérer la sécurité des accès à votre réseau de manière centralisée et ce depuis votre console **Network Policy Server**.


Serveur NPS (Network Policy Server)
Fichier
Action
Affichage
?
NPS (Local)
Clients et serveurs RADIUS
Stratégies
Stratégies de demande de connexion
Stratégies réseau
Stratégies de contrôle d'intégrité
Protection d'accès réseau
Gestion
Mise en route
Le serveur NPS (Network Policy Server) vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'intégrité des clients, ainsi que sur l'authentification et l'autorisation des demandes de connexion.
Configuration standard
Sélectionnez un scénario de configuration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.
Protection d'accès réseau (NAP)
Protection d'accès réseau (NAP)
Lorsque vous configurez un serveur NPS (Network Policy Server) en tant que serveur de stratégie NAP, vous créez des stratégies de contrôle d'intégrité qui permettent au serveur NPS de valider la configuration des ordinateurs clients compatibles avec la protection d'accès réseau (NAP) avant qu'ils ne se connectent à votre réseau. Les clients qui ne sont pas conformes à la stratégie de contrôle d'intégrité peuvent être placés sur un réseau restreint et être automatiquement mis à jour afin de répondre aux exigences de conformité.
Configurer la protection d'accès réseau (NAP)
Informations
Configuration avancée

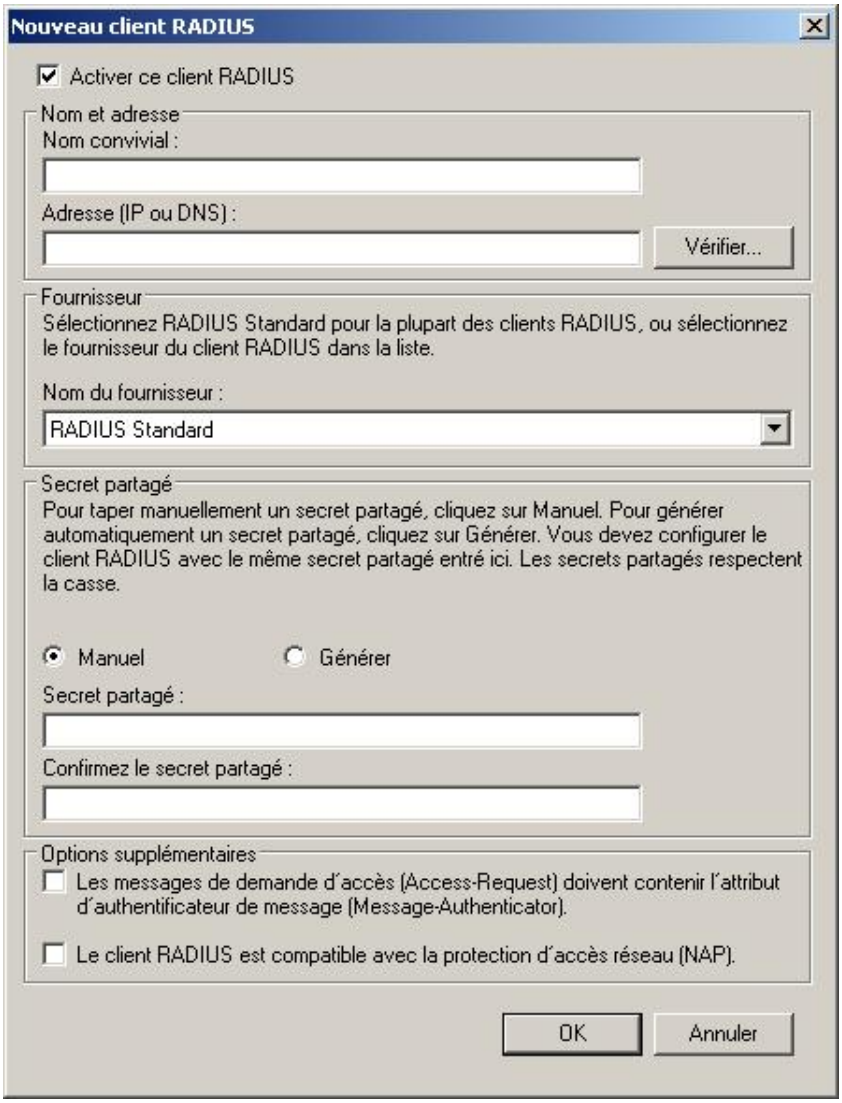
La configuration des stratégies d'accès (horaires, utilisateurs, etc.) se fait de la même façon que pour un serveur VPN (vu précédemment dans ce même chapitre). Vous pouvez cependant désormais configurer votre serveur NPS de sorte à agir en temps que serveur RADIUS ou encore en temps que Proxy RADIUS.

Pour permettre à un périphérique d'accès d'utiliser votre serveur en temps que serveur RADIUS il vous faut au préalable l'avoir autorisé. Pour ce faire voici comment procéder :

- Dans votre console NPS, naviguez jusqu'à **Clients et Serveurs RADIUS**.

- Faites un clic avec le bouton droit de la souris sur **Clients RADIUS** puis **Nouveau**.

© ENI Editions - All rigths reserved


Nouveau client RADIUS
Activer ce client RADIUS
Nom et adresse
Nom convivial :
Adresse (IP ou DNS) :
Vérifier...
Fournisseur
Sélectionnez RADIUS Standard pour la plupart des clients RADIUS, ou sélectionnez le fournisseur du client RADIUS dans la liste.
Nom du fournisseur :
RADIUS Standard
Secret partagé
Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.
Manuel
Générer
Secret partagé :
Confirmez le secret partagé :
Options supplémentaires
Les messages de demande d'accès (Access-Request) doivent contenir l'attribut d'authentificateur de message (Message-Authenticator).
Le client RADIUS est compatible avec la protection d'accès réseau (NAP).
OK
Annuler

- Il vous suffit alors de déclarer le périphérique d'accès en lui donnant un **Nom convivial** et son **Adresse IP**.

  Le **Nom du fournisseur** (la liste déroulante fournit de nombreux acteurs importants du monde informatique comme Cisco, etc.).

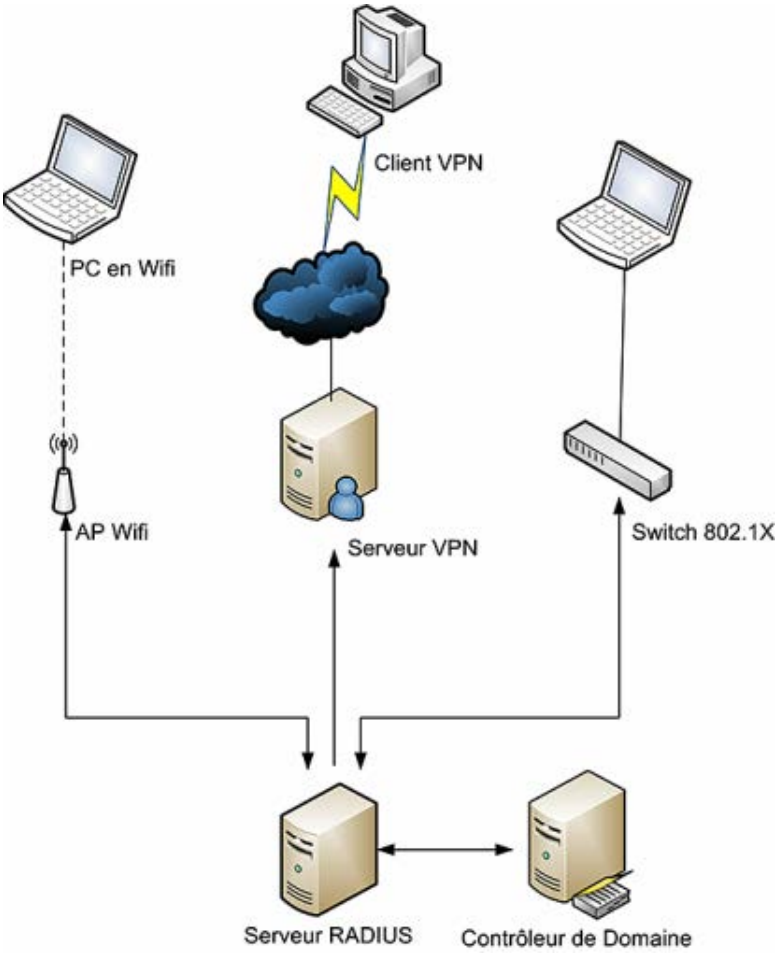
  Une clé de sécurité que vous configurerez également sur le périphérique d'accès.

  Vous pourrez également choisir les protocoles d'authentification ainsi que spécifier si le client RADIUS est compatible NAP ou non.

Une fois un périphérique déclaré, vous pouvez l'activer ou le désactiver par un simple clic droit et une case à cocher. Pour ce faire, il suffit dans la rubrique **Clients RADIUS**, d'aller dans les propriétés du périphérique nouvellement créé. Il ne vous reste alors qu'à choisir entre **Activé** ou **Désactivé**.

Ci-dessous, un exemple d'utilisation de serveur Radius.

© ENI Editions - All rigths reserved



Il peut être intéressant d'utiliser un serveur Proxy RADIUS dans les cas suivants :

- Vous voulez fournir une authentification pour des comptes non membres du domaine dont fait partie le serveur NPS.
- Vous voulez fournir une authentification depuis une base de comptes autre que Windows.
- Vous voulez pouvoir traiter un grand nombre de requêtes de connexion. Le Proxy RADIUS agira comme un équilibreur de charge.
- Vous voulez sécuriser l'accès à votre base d'utilisateurs en plaçant un proxy RADIUS en DMZ.

Déclarer votre serveur en temps que Serveur proxy RADIUS est également très simple. Il vous suffit dans votre console NPS de :

- Naviguer jusqu'à **Clients et serveurs RADIUS**.
- Faire un clic droit sur **Groupes de serveurs RADIUS distants** puis **Nouveau**.
- Spécifier un nom de groupe puis cliquez sur **Ajouter**.
- Entrer le nom ou l'adresse IP d'un serveur RADIUS.
- Vous pourrez également spécifier si le proxy RADIUS doit s'authentifier via une clé partagée auprès du serveur RADIUS, ou encore configurer l'équilibrage de charge.
- Il vous est possible dans un même groupe d'ajouter plusieurs serveurs RADIUS afin d'assurer une tolérance de pannes.

© ENI Editions - All rigths reserved

Vous venez de voir dans ce chapitre que pour fournir un accès à distance à vos utilisateurs, il vous faut configurer un serveur d'accès distants. Quand vos utilisateurs se trouvent en dehors de l'entreprise ils peuvent accéder aux ressources internes en utilisant soit une connexion de type Dial-up, soit une connexion VPN.

Windows 2008 sait gérer les deux solutions. Il apporte également avec SSTP une mobilité accrue. Grâce à l'encapsulation du trafic VPN dans de l'HTTPS vous évitez les contraintes de connexion liées à de la sécurité sortante sur les pare-feu des réseaux dans lesquels vous vous situez. Windows 2008 vous permet également avec ses nouvelles stratégies d'accès, de définir de façon très précise qui se connecte, quand et de quelle façon.

Si vous souhaitez centraliser la sécurité des connexions de vos équipements réseaux, Windows Server 2008 assurera le rôle de concentrateur grâce à ses fonctions RADIUS.

© ENI Editions - All rigths reserved

Mettre en place un serveur Intranet/Internet

Dans ce chapitre vous apprendrez à installer et configurer un serveur Web grâce au rôle de serveur IIS (*Internet Information Services*).

1. Présentation d'IIS7

a. Présentation générale

IIS7 (*Internet Information Services*) est la dernière version du serveur Web de Microsoft. Inclus en version complète avec Windows Server 2008, il fournit une plate-forme sécurisée et facile à administrer pour pouvoir héberger des Services Web ainsi que des applications Web enrichies.

Dans cette 7e version, IIS permet d'héberger et de gérer la plupart des langages utilisés sur le Web allant de l'ASP.net au PHP. Sa rétrocompatibilité permet de migrer aisément vos sites Web hébergés sur les versions précédentes de IIS sans rencontrer de problème.

IIS7 offre des fonctionnalités différentes en fonction du système d'exploitation. Tout comme IIS6, il peut être installé sur le système d'exploitation client (Windows Vista) en version allégée. Windows Vista et Windows Server 2008 partageant le même noyau, il est donc facile de développer des applications depuis son poste de travail pour ensuite les faire héberger par un serveur. Décliné en édition Web, Windows Web Server 2008 propose lui aussi une plate-forme Web complète basée sur IIS7. Moins cher que les autres éditions, Windows Web Server 2008 supporte jusqu'à 32 Go de mémoire vive (sur un système non 32-bits, qui est limité à 4 Go) et jusqu'à 4 processeurs.

IIS7 peut également être installé en mode Core mais il faut garder à l'esprit qu'aucun site développé en ASP.Net ne pourra être publié dans ce cas. En effet, le mode Core de Windows Server 2008 ne permet pas l'installation du .Net Framework pour des raisons de sécurité. Cependant, sachez qu'il est possible d'installer le .Net Framework 2.0 et 3.0 en mode Core sur un Windows Server 2008 R2. La version R2 permet également d'installer un FTP sécurisé et les fonctionnalités Webdav.

b. Nouvelle architecture

L'architecture d'IIS a été repensée afin de faciliter l'implémentation des fonctionnalités et donc l'extension des possibilités du serveur. Sous IIS6, la structure était composée d'un seul bloc ce qui obligeait à tout installer pour utiliser le serveur Web. Avec IIS7, les fonctionnalités ont été découpées de façon à pouvoir charger les modules en correspondance avec les besoins.

Ces modules sont découpés en cinq catégories pour la partie **Serveur Web**.

- Fonctionnalités HTTP communes (contenu statique, documents par défaut, etc.).
- Développement d'applications (prise en charge de : ASP.Net, ASP, CGI, etc.).
- Intégrité et diagnostics (journalisation, observateur de demandes, suivi, etc.).
- Sécurité (authentification de base, authentification Windows, autorisation Digest, etc.).
- Performances (Compression de contenu statique ou dynamique).

Pour la partie **Outils de gestion**, on retrouve :

- la console de gestion de IIS ;
- les scripts et outils de gestion de IIS ;
- le service de gestion ;
- la gestion de la compatibilité avec IIS6.

Le service FTP (*File Transfer Protocol*) est séparé de la partie serveur Web car il s'agit désormais d'un service de rôle à part entière. Les modules Serveur FTP et Console de gestion FTP lui sont associés.

© ENI Editions - All rigths reserved

c. Nouvelle administration

IIS7 diffère de sa version précédente par la mise en place d'une nouvelle administration. La nouvelle console de gestion qui centralise l'administration de l'ensemble des modules du serveur n'est plus un simple composant enfichable. En effet, il s'agit d'une console à part entière qui se connecte sur le service d'administration.

La configuration a également changé. Sous IIS6, elle était stockée dans une métabase au format XML. IIS7 facilite l'implémentation et surtout la maintenance des serveurs, en découpant cette configuration dans plusieurs fichiers XML :

- **applicationHost.config** : contient la configuration globale (liste des sites, pools d'applications, paramètres par défaut, etc.).
- **Redirection.config** : contient les informations de redirection (utilisé par exemple quand le contenu du site se trouve sur un autre serveur ou encore lorsqu'une partie du site ne doit pas être disponible en cas de maintenance, etc.).
- **Web.config** : contient la configuration globale ASP.Net du serveur (un fichier individuel peut être créé pour chaque site qui a besoin d'une configuration spécifique. Ceci est utile lorsque vous devez spécifier des paramètres différents de la configuration globale du serveur). Cela permet ainsi de gérer plus finement les paramétrages de sites Web.
- **Machine.config** : contient les propriétés requises pour les fonctionnalités Framework.

---

applicationHost.config et redirection.config sont stockés à l'emplacement : %windir%\system32\inetsrv\config. Le fichier web.config de premier niveau est lui situé à l'emplacement : c:\inetpub\wwwroot. Autrement, les fichiers web.config et machine.config se trouvent dans le dossier %windir%\Microsoft.NET\Framework\version_framework\CONFIG.

Il existe avec ces différents fichiers de configuration une hiérarchie. Celle-ci définit un héritage des paramètres tout comme le feraient des droits de sécurité NTFS. Cette hiérarchie commence par le fichier **machine.config** puis suit l'ordre : **web.config** (celui de premier niveau) ; **applicationHost.config** et enfin un fichier web.config optionnel situé à l'emplacement du site ou du répertoire virtuel. De cette façon, les propriétés sont héritées du fichier **machine.config** au dernier fichier **web.config** de l'arborescence.

Le stockage de la configuration des sites dans des fichiers XML distincts (aussi appelée configuration distribuée) permet ainsi de faciliter le déploiement ou la copie d'applications. Vous pouvez copier les applications entre des serveurs frontaux grâce à un simple *xcopy* en évitant toute erreur due à une réplication ou une quelconque synchronisation.

Les tâches administratives sont désormais automatisables grâce notamment à Powershell, un nouveau fournisseur WMI, une nouvelle API .Net mais surtout grâce à l'outil AppCMD.AppCMD.exe permet de réaliser la majorité des tâches d'administration à l'aide d'une syntaxe simple.

L'administration peut également être déléguée. Vous pouvez spécifier quelles sont les fonctionnalités que les utilisateurs non administrateurs sont en mesure de gérer. Il est ainsi possible par exemple de configurer les paramètres ASP.net d'un site sans pour autant devoir le faire avec des privilèges administrateur.

2. Installation du rôle Serveur Web (IIS) en mode console

Avant que vous vous lanciez dans l'installation, il est important que vous connaissiez la liste des modules non disponibles avec le mode Core :

- IIS-ASPNET ;
- IIS-NetFxExtensibility ;
- IIS-ManagementConsole ;
- IIS-ManagementService ;
- IIS-LegacySnapIn ;

© ENI Editions - All rigths reserved

- IIS-FTPManagement ;
- WAS-NetFxEnvironment ;
- WAS-ConfigurationAPI.

En mode Core, la version R2 de Windows Server 2008 supporte les composants .NET Framework et ASP.Net. Pour installer IIS en mode Core il vous faut utiliser l'exécutable **pkgmgr.exe**.

Pour réaliser une installation par défaut, utilisez la commande ci-dessous :

```
start /w pkgmgr /iu:IIS-WebServerRole;WAS-
WindowsActivationService;WAS-ProcessModel
```

Pour réaliser une installation complète sur un serveur Core, utilisez la commande suivante :

```
start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-
CommonHttpFeatures;IIS-StaticContent;IIS-
DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-
HttpRedirect;IIS-ApplicationDevelopment;IIS-ASP;IIS-
CGI;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-
ServerSideIncludes;IIS-HealthAndDiagnostics;IIS-
HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-
HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IIS-
Security;IIS-BasicAuthentication;IIS-
WindowsAuthentication;IIS-DigestAuthentication;IIS-
ClientCertificateMappingAuthentication;IIS-
IISCertificateMappingAuthentication;IIS-
URLAuthorization;IIS-RequestFiltering;IIS-IPSecurity;IIS-
Performance;IIS-HttpCompressionStatic;IIS-
HttpCompressionDynamic;IIS-WebServerManagementTools;IIS-
ManagementScriptingTools;IIS-
IIS6ManagementCompatibility;IIS-Metabase;IIS-
WMICompatibility;IIS-LegacyScripts;IIS-
FTPPublishingService;IIS-FTPServer;WAS-
WindowsActivationService;WAS-ProcessModel
```

Vous pourrez vérifier que le rôle a bien été installé en utilisant la commande `oclist`. En la lançant vous verrez la liste des rôles de serveur disponibles. Pour chacun d'eux vous verrez mentionné *Installé* ou *Non Installé*. Pour les serveurs de rôle installés, un sous-arbre est représenté avec l'état d'installation de chaque service de rôle.

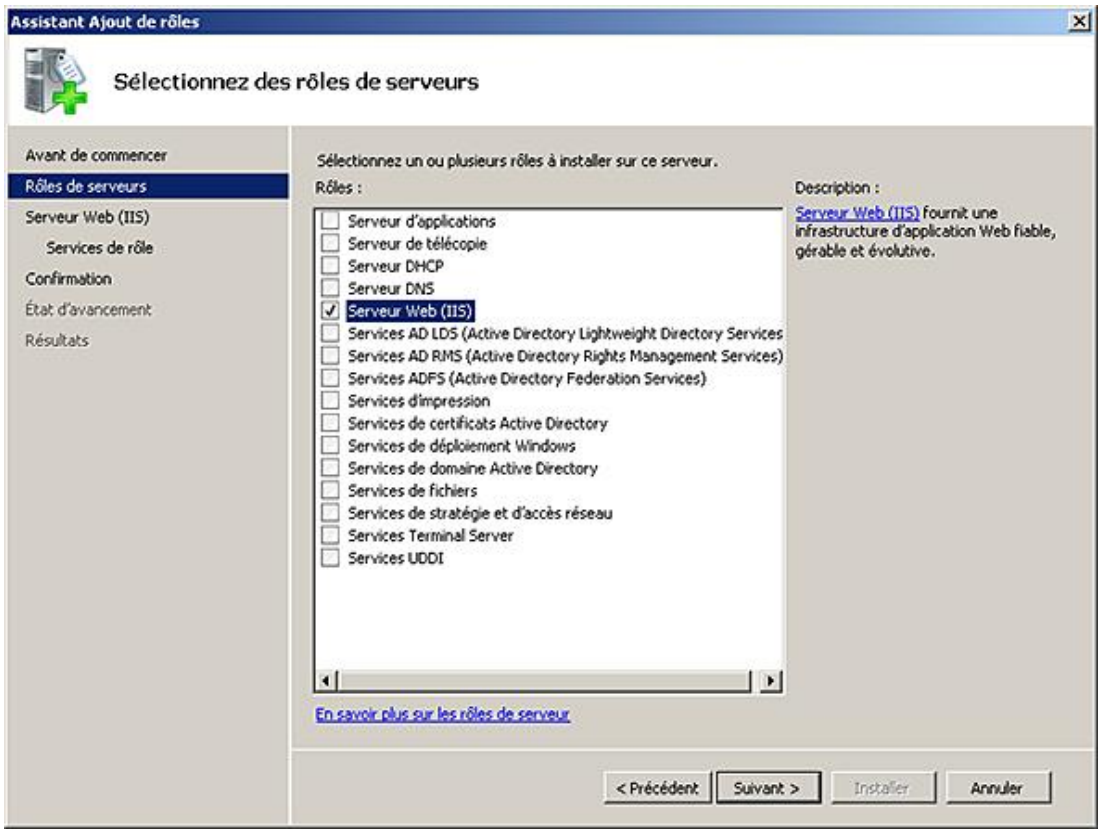
3. Installation du rôle Serveur Web (IIS) en mode graphique

L'installation du rôle se fait depuis la console **Gestionnaire de Serveur**, dans le sous-dossier **Rôles**, en cliquant sur **Ajouter des rôles**.

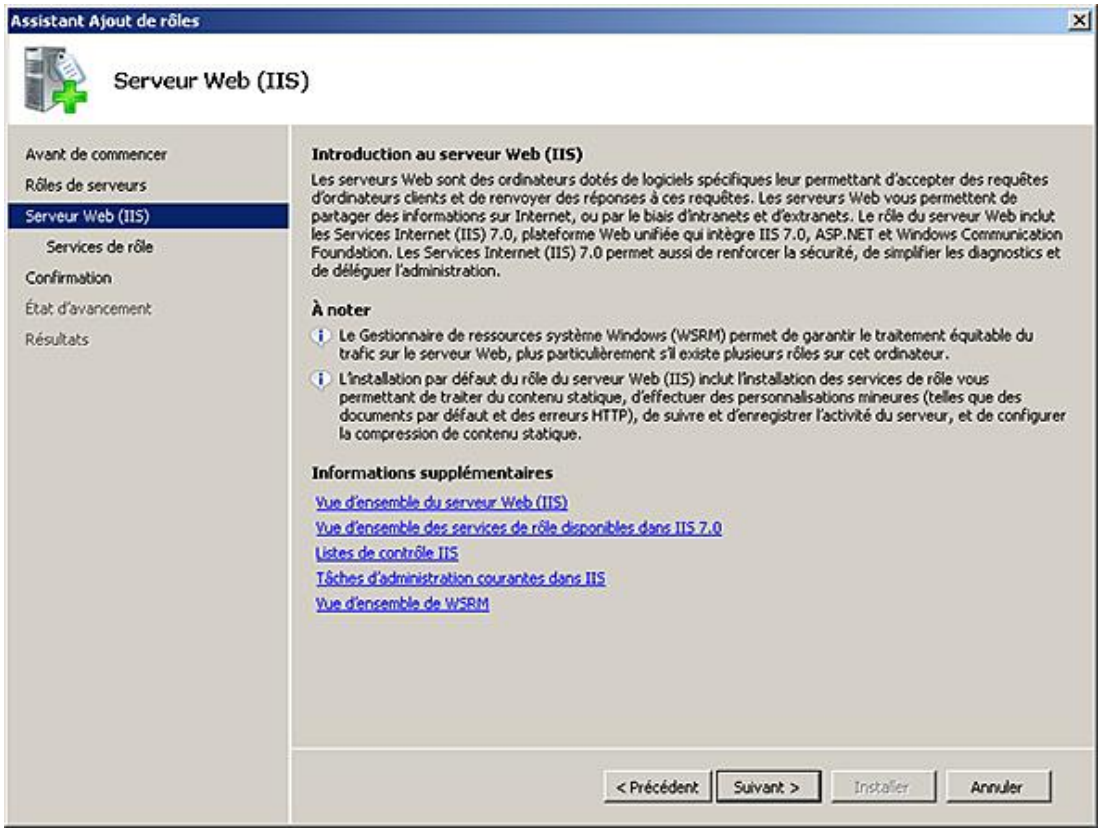
Voici les différentes étapes :

- Ouvrez la console **Gestionnaire de serveur** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Gestionnaire de serveur**.
- Au niveau de **Résumé des rôles**, cliquez sur **Ajouter des rôles**.
- Cliquez sur **Suivant**.
- Cochez la case **Serveur Web (IIS)** comme ci-dessous puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved

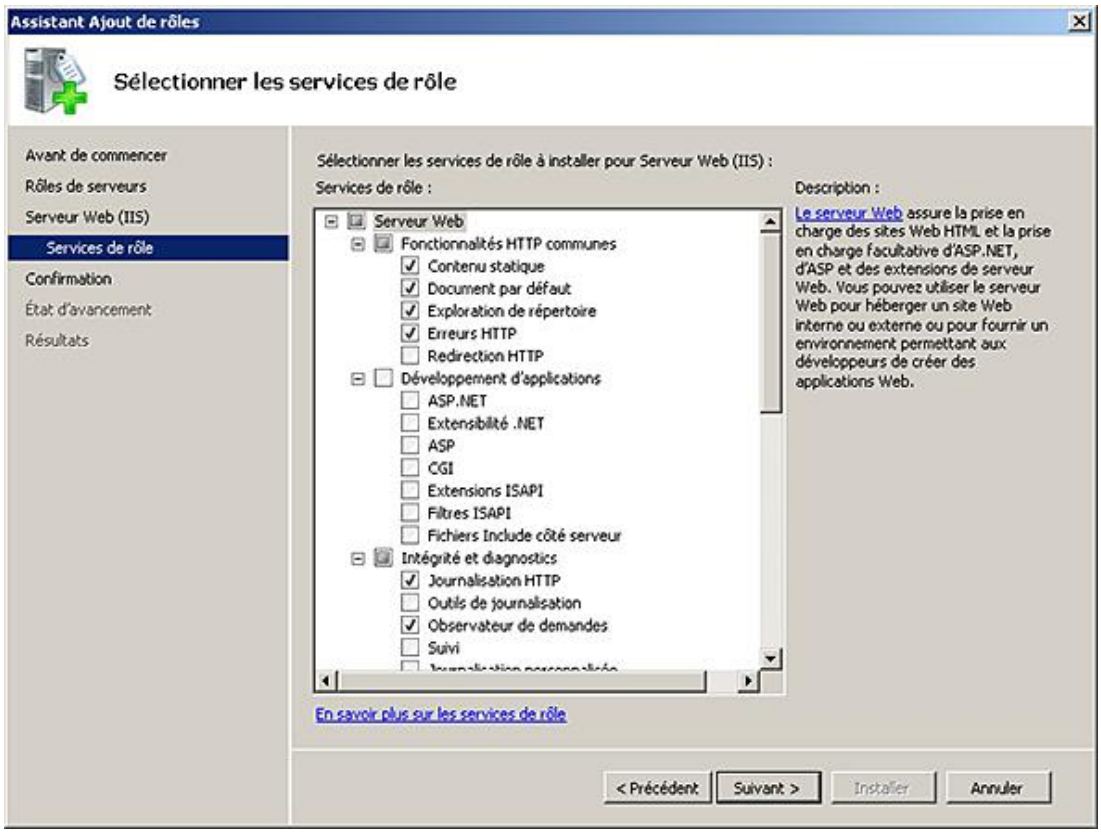


- Lisez la page d'introduction puis cliquez sur **Suivant**.

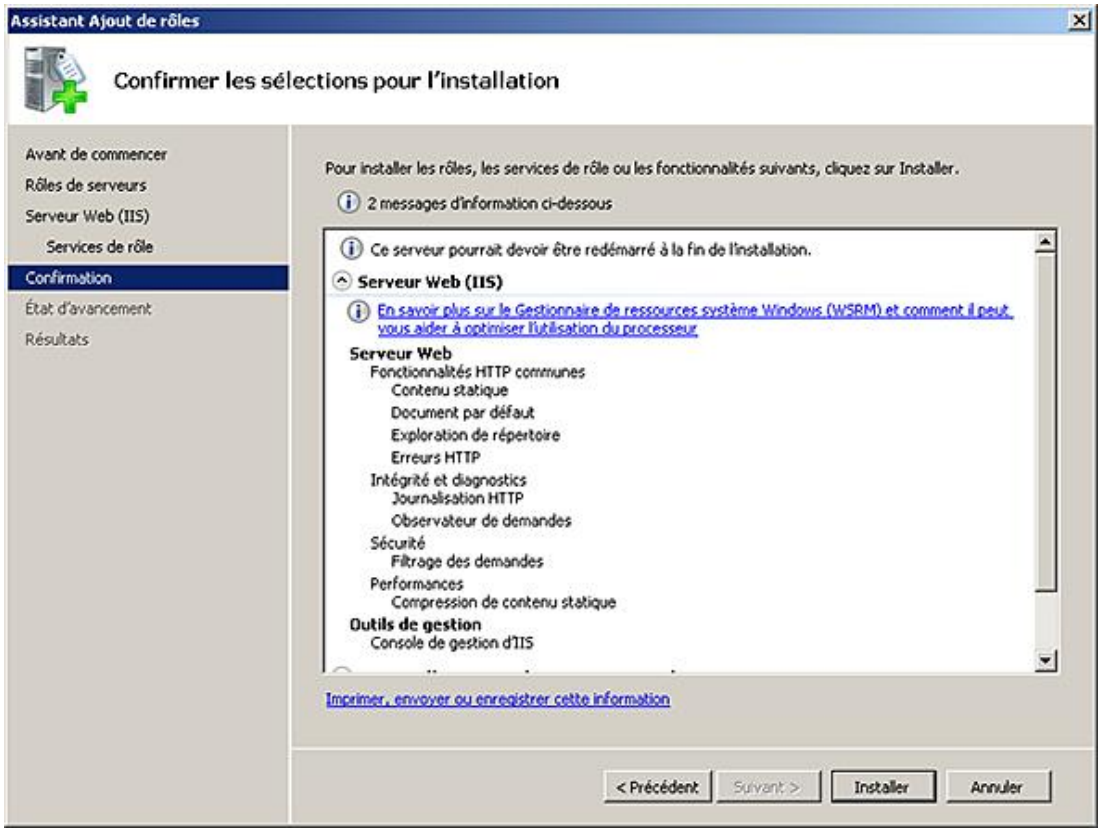

Assistant Ajout de rôles
Serveur Web (IIS)
Avant de commencer
Rôles de serveurs
Serveur Web (IIS)
Services de rôle
Confirmation
État d'avancement
Résultats
Introduction au serveur Web (IIS)
Les serveurs Web sont des ordinateurs dotés de logiciels spécifiques leur permettant d'accepter des requêtes d'ordinateurs clients et de renvoyer des réponses à ces requêtes. Les serveurs Web vous permettent de partager des informations sur Internet, ou par le biais d'intranets et d'extranets. Le rôle du serveur Web inclut les Services Internet (IIS) 7.0, plateforme Web unifiée qui intègre IIS 7.0, ASP.NET et Windows Communication Foundation. Les Services Internet (IIS) 7.0 permet aussi de renforcer la sécurité, de simplifier les diagnostics et de déléguer l'administration.
À noter
Le Gestionnaire de ressources système Windows (WSRM) permet de garantir le traitement équitable du trafic sur le serveur Web, plus particulièrement s'il existe plusieurs rôles sur cet ordinateur.
L'installation par défaut du rôle du serveur Web (IIS) inclut l'installation des services de rôle vous permettant de traiter du contenu statique, d'effectuer des personnalisations mineures (telles que des documents par défaut et des erreurs HTTP), de suivre et d'enregistrer l'activité du serveur, et de configurer la compression de contenu statique.
Informations supplémentaires
Vue d'ensemble du serveur Web (IIS)
Vue d'ensemble des services de rôle disponibles dans IIS 7.0
Listes de contrôle IIS
Tâches d'administration courantes dans IIS
Vue d'ensemble de WSRM
< Précédent
Suivant >
Installer
Annuler

- Dans l'exemple en cours, vous n'utiliserez que les fonctions de base de IIS. Laissez les cases par défaut cochées puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved

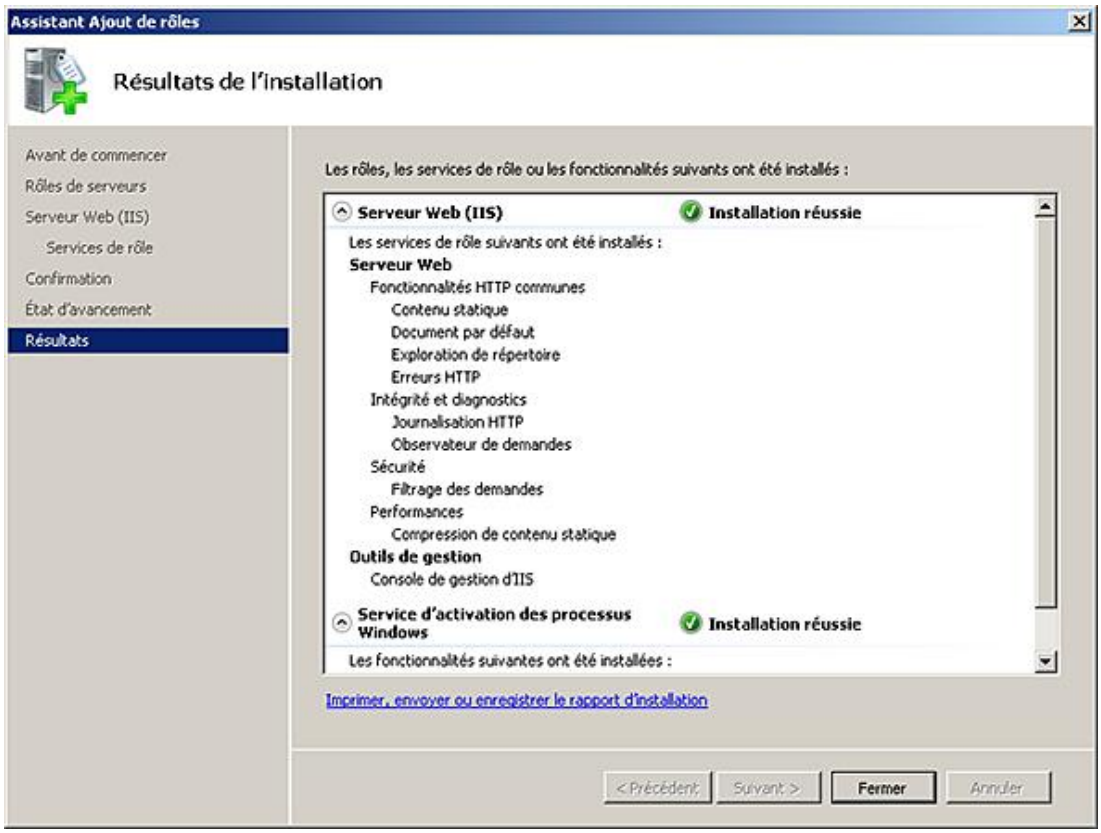

Assistant Ajout de rôles
Sélectionner les services de rôle
Avant de commencer
Rôles de serveurs
Serveur Web (IIS)
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Serveur Web (IIS) :
Services de rôle :
Description :
Serveur Web
Fonctionnalités HTTP communes
Contenu statique
Document par défaut
Exploration de répertoire
Erreurs HTTP
Redirection HTTP
Développement d'applications
ASP.NET
Extensibilité .NET
ASP
CGI
Extensions ISAPI
Filtres ISAPI
Fichiers Include côté serveur
Intégrité et diagnostics
Journalisation HTTP
Outils de journalisation
Observateur de demandes
Suivi
Le serveur Web assure la prise en charge des sites Web HTML et la prise en charge facultative d'ASP.NET, d'ASP et des extensions de serveur Web. Vous pouvez utiliser le serveur Web pour héberger un site Web interne ou externe ou pour fournir un environnement permettant aux développeurs de créer des applications Web.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler

- Vérifiez les options choisies puis cliquez sur **Installer**.


Assistant Ajout de rôles
Confirmer les sélections pour l'installation
Avant de commencer
Rôles de serveurs
Serveur Web (IIS)
Services de rôle
Confirmation
État d'avancement
Résultats
Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer.
2 messages d'information ci-dessous
Ce serveur pourrait devoir être redémarré à la fin de l'installation.
Serveur Web (IIS)
En savoir plus sur le Gestionnaire de ressources système Windows (WSRM) et comment il peut vous aider à optimiser l'utilisation du processeur
Serveur Web
Fonctionnalités HTTP communes
Contenu statique
Document par défaut
Exploration de répertoire
Erreurs HTTP
Intégrité et diagnostics
Journalisation HTTP
Observateur de demandes
Sécurité
Filtrage des demandes
Performances
Compression de contenu statique
Outils de gestion
Console de gestion d'IIS
Imprimer, envoyer ou enregistrer cette information
< Précédent
Suivant >
Installer
Annuler

- Vérifiez que l'installation s'est bien déroulée puis cliquez sur **Fermer**.

© ENI Editions - All rigths reserved



- Pour vérifier que IIS7 est bien opérationnel, ouvrez Internet Explorer puis dans la barre d'adresse saisissez l'url : http://localhost

  Vous devriez voir apparaître la fenêtre suivante :

© ENI Editions - All rigths reserved

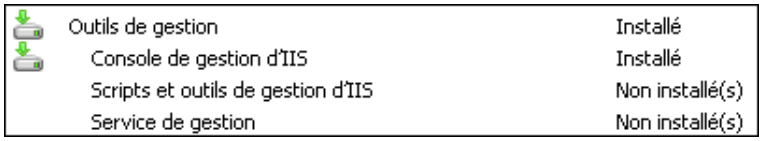
© ENI Editions - All rigths reserved

Monter un site Web

Maintenant que vous avez installé votre rôle de **Serveur Web (IIS)**, vous allez voir comment créer de nouveaux sites et les gérer facilement. Dans ce chapitre vous configurerez un site pour votre société (le contenu du site sera minimal, le but de ce livre n'étant pas de vous formez aux langages de développement Web).

1. Création et configuration d'un site

Avec Windows Server 2008, la gestion de IIS se fait depuis une console dédiée. Ainsi si vous regardez dans votre **Gestionnaire de Serveur**, dans la section **Services de rôle de IIS** vous pouvez voir le service **Console de gestion d'IIS**.

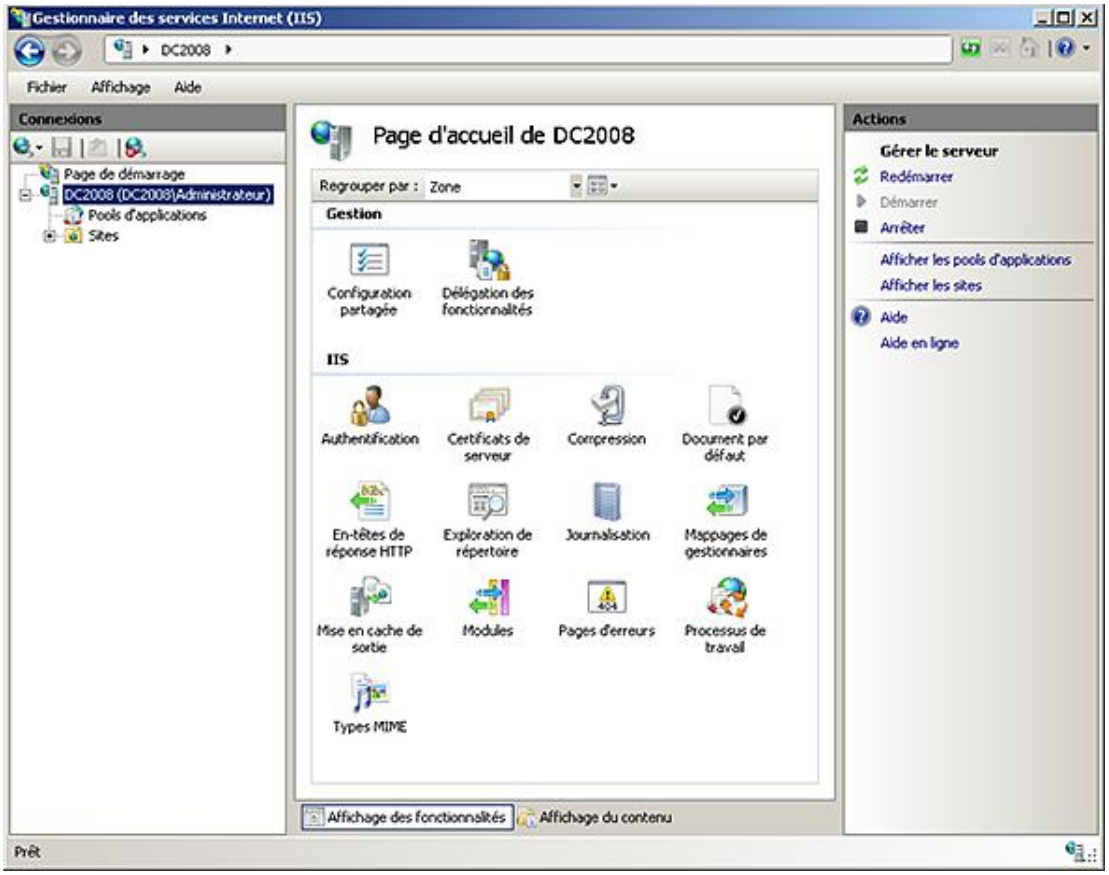

Outils de gestion Installé
Console de gestion d'IIS Installé
Scripts et outils de gestion d'IIS Non installé(s)
Service de gestion Non installé(s)

Pour atteindre cette console :

- Allez dans **Démarrer - Tous les Programmes - Outils d'administration** et cliquez sur **Gestionnaire de services Internet (IIS)**.

  Par défaut la console de gestion de IIS se connecte au serveur local. Cela vous permet de changer la configuration et les paramètres de ce serveur.

- Dans le volet de gauche, cliquez ensuite sur le nom de votre serveur (ici DC2008) pour faire apparaître la liste des fonctionnalités disponibles.



Par défaut, l'affichage regroupe les fonctionnalités par **Zone**. Vous pouvez changer cet affichage grâce à la liste déroulante située en haut du volet central. Il est ainsi possible de regrouper par **Zone** (par défaut), par **Catégorie** ou encore de ne pas utiliser de regroupage.

© ENI Editions - All rigths reserved

Voici les différentes étapes pour créer un nouveau site :

Pré-requis : vous devez avoir créé un répertoire *Société* dans le dossier **C:\inetpub\wwwroot**.

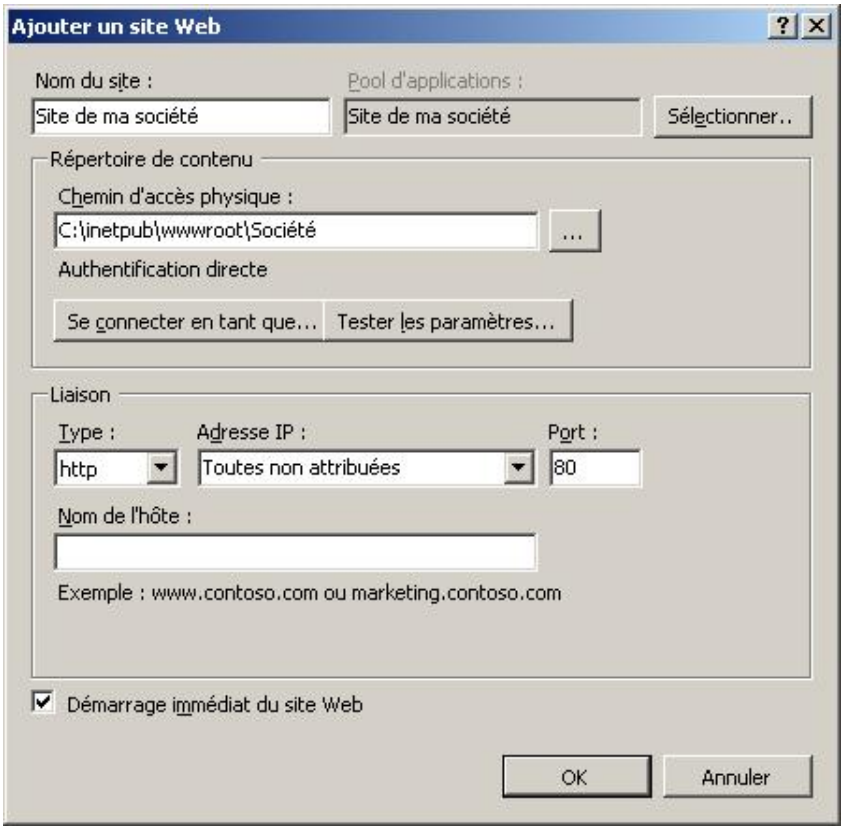
- Toujours dans la console **Gestionnaire des services Internet (IIS)**, faites un clic avec le bouton droit de la souris sur le nom de votre serveur puis cliquez sur **Ajouter un site Web**.

  (la même opération peut être réalisée depuis plusieurs endroits. Par exemple directement depuis la sous-arborescence **Sites**).

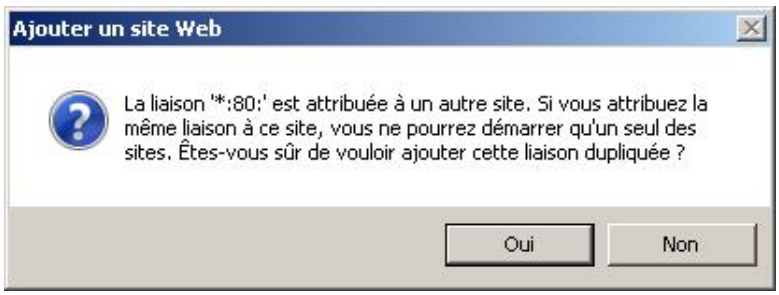
- Remplissez la fenêtre comme ci-dessous.

  Le nom du site est purement informatif, les espaces ne poseront pas de problème à l'utilisation

  Dans cet exemple, ne remplissez pas le nom de l'hôte et laissez les paramètres de liaison par défaut. Ces paramètres de liaison servent à définir sur quel port et/ou par quel nom vous accédez au site (vous trouverez plus de détails dans la sous-partie suivante de ce chapitre).



- Une fois les champs remplis cliquez sur **OK**, le message suivant apparaît :


Ajouter un site Web
La liaison '*:80:' est attribuée à un autre site. Si vous attribuez la même liaison à ce site, vous ne pourrez démarrer qu'un seul des sites. Êtes-vous sûr de vouloir ajouter cette liaison dupliquée ?
Oui
Non

La raison de ce message est que IIS héberge déjà un site utilisant le port 80 sur la même adresse IP. Il s'agit du site Web par défaut. Il n'est pas possible pour une seule adresse IP et un seul port d'avoir plusieurs sites Web (sauf utilisation des en-têtes HTTP. Ce point est abordé dans la section suivante de ce chapitre).

Si vous essayez tout de même de démarrer le site Web vous serez confronté à un message d'erreur. Pour le

© ENI Editions - All rigths reserved

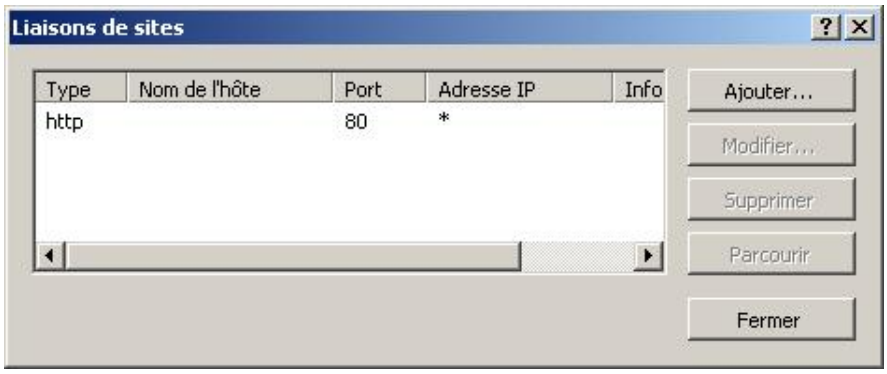
constater, suivez la procédure ci-après :

- Dans le volet central, sélectionnez votre site Web puis dans le volet de droite cliquez sur le bouton **Démarrer**. Vous obtenez le message ci-dessous.

Pour les besoins de l'exemple, vous allez changer le port sur lequel ce site Web va écouter.

- Dans le volet de gauche, étendez l'arborescence **Sites** pour faire apparaître le site que vous venez de créer puis sélectionnez-le.

- Dans le volet de droite, dans la rubrique **Actions**, cliquez sur **Liaisons**.



- Sélectionnez la liaison HTTP puis cliquez sur **Modifier**.

- Saisissez **8080** dans le champ **Port** puis cliquez sur **OK** pour valider puis sur **Fermer**.

- Il vous faut désormais un document à afficher dans votre site. Pour le créer, ouvrez l'éditeur Notepad puis saisissez le code suivant :

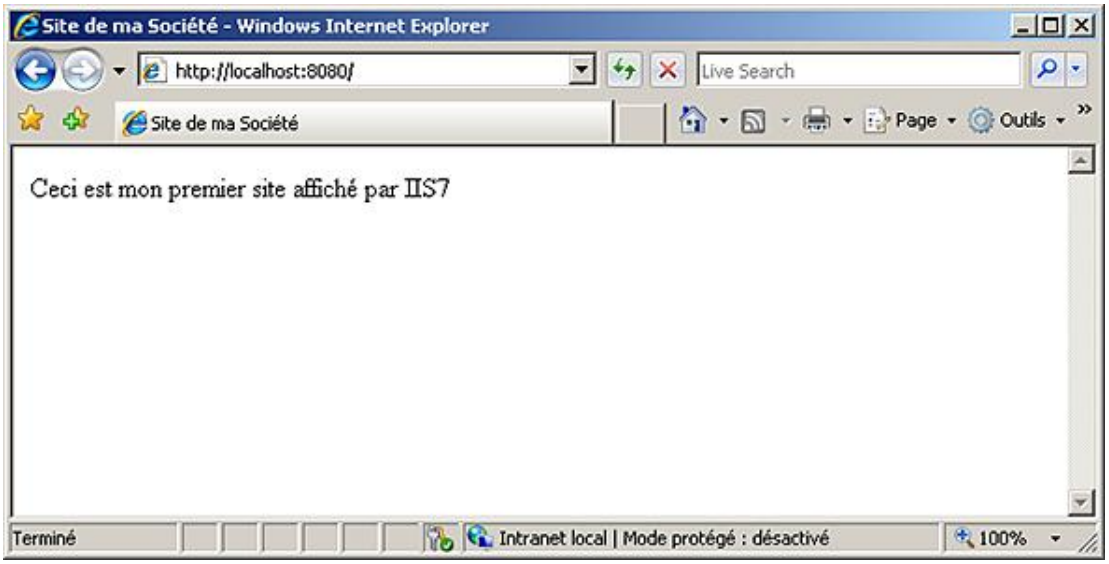
```
<HTML>
<head>
    <Title>Site de Ma société</Title>
</head>
```

© ENI Editions - All rigths reserved

```
<body>
    Ceci est mon premier site affiché par IS7
</body>
</HTML>
```

- Enregistrez ensuite le fichier à l'emplacement : c:\inetpub\wwwroot\Société\default.htm

- Pour tester le fonctionnement, ouvrez Internet Explorer puis saisissez l'adresse http://localhost:8080



2. Mise à jour du domaine DNS

Bien que l'on puisse utiliser des ports d'écoute différents pour chaque site, dans la pratique ce n'est pas une solution viable lorsque plusieurs sites sont hébergés sur un même serveur. Ce problème se pose tout particulièrement pour des sites Web publics. Les internautes ne savent pas sur quel port est configuré votre site Web et il n'est donc pas envisageable de leur demander d'indiquer un port particulier afin de pouvoir accéder à votre site Internet.

Une des solutions permettant de contourner ce problème de ports est de configurer plusieurs adresses IP sur votre serveur Web. Chaque IP est ensuite associée à un site unique. Si cette solution peut faire l'affaire pour une utilisation interne, elle se révèle très coûteuse pour une utilisation publique (les adresses IP fixes sur Internet représentent un investissement et sont fournies en quantité limitée).

Pour pouvoir gérer de façon efficace l'hébergement de nombreux sites Web, il vous faut faire appel aux **en-têtes d'hôte**. Ces en-têtes d'hôte permettent l'utilisation de plusieurs noms d'hôtes pour une seule adresse IP. IIS va écouter les demandes entrantes et regarder les informations envoyées par le navigateur. En fonction du nom d'hôte reçu, il redirige la requête du navigateur vers le site Web correspondant.

Vous allez dans l'exemple qui suit configurer le site créé à l'étape précédente pour écouter sur l'adresse www.masociete.fr

Pré-requis : avoir un serveur DNS fonctionnel qui héberge la zone masociete.fr. Avoir dans cette zone un enregistrement de type A appelé **www** et qui pointe sur l'IP 192.168.0.1 (l'adresse IP de votre serveur web).

Consultez le chapitre Mise en place des services réseaux d'entreprise - Mise en place des systèmes de résolutions de nom.

- Allez dans la console **Gestionnaire des services Internet (IIS)**.

- Développez l'arborescence **Sites** pour faire apparaître le site créé lors de la sous-partie précédente de ce chapitre (Site de ma société).

- Sélectionnez votre site puis dans le volet de droite cliquez sur **Liaisons**.

- Dans la fenêtre **Liaisons de sites** cliquez sur **Ajouter**.

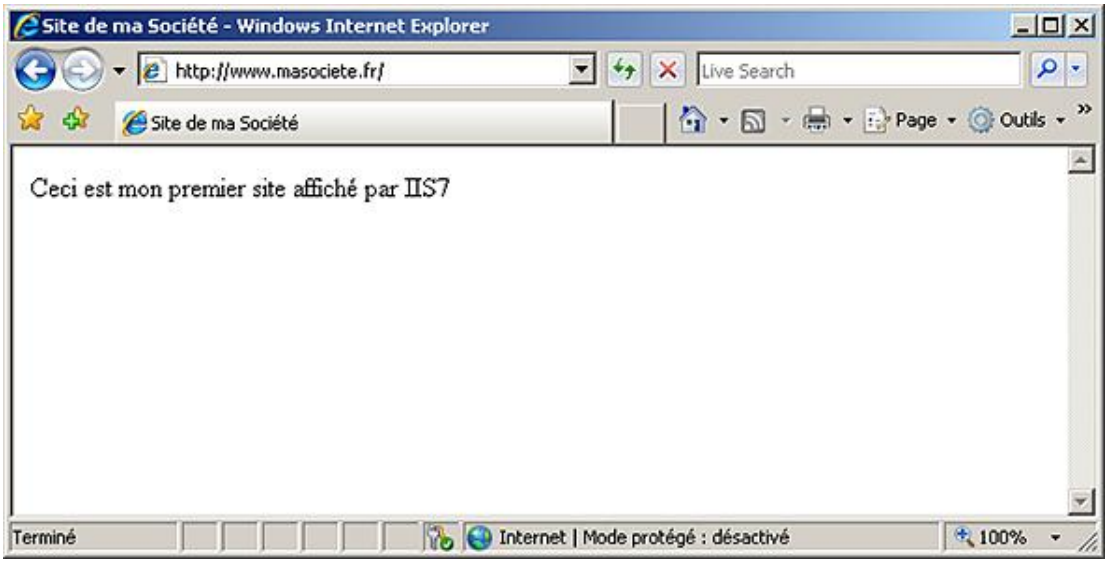
© ENI Editions - All rigths reserved

- Remplissez les champs comme ci-dessous :

- Validez en cliquant sur **OK** puis sur **Fermer**.

Vous pouvez tout aussi bien modifier la liaison existante pour spécifier ces paramètres. Cependant grâce à cet exemple vous constatez que l'on peut affecter des ports différents sur un même site et même des noms d'hôte différents.

- Testez ensuite la modification en ouvrant Internet Explorer puis saisissez l'adresse www.masociete.fr dans la barre d'adresse et validez.



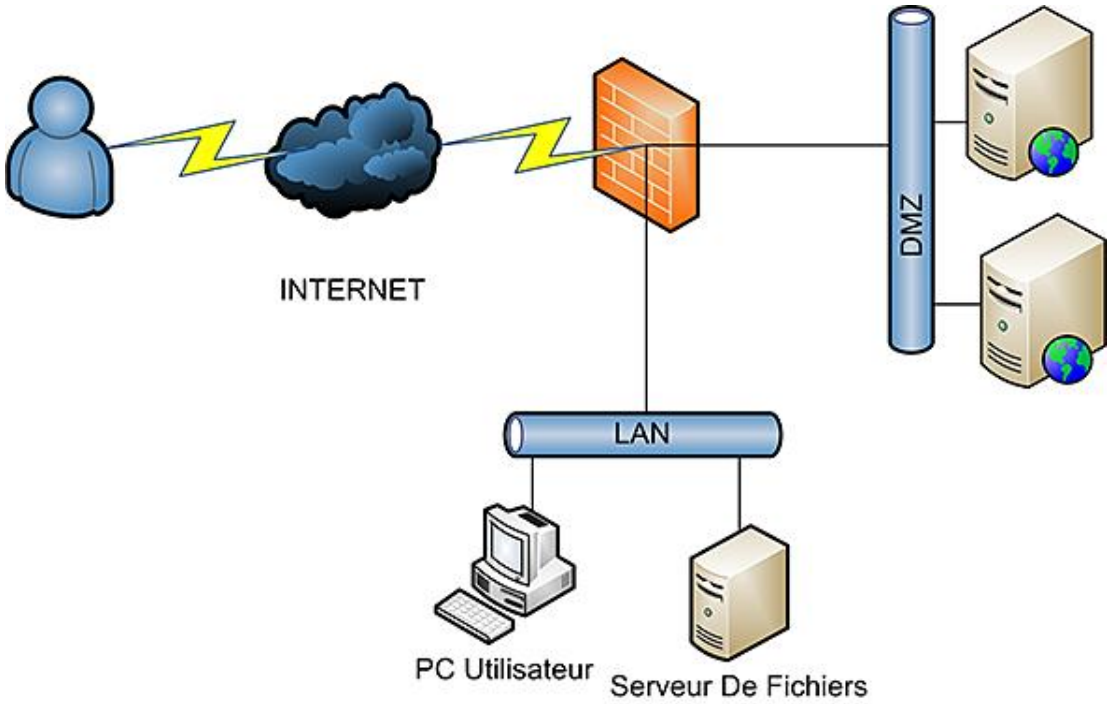
Chaque nom d'hôte que vous souhaitez utiliser pour IIS a besoin d'exister. Pour un site intranet, il vous suffit de rajouter des enregistrements dans votre zone DNS de domaine. Pour une utilisation publique, il vous faut le gérer sur la zone DNS publique. Soit vous avez accès à une interface d'administration qui vous le permet, soit vous devez demander au gestionnaire de votre zone DNS de créer les enregistrements en conséquence.

3. Mise en place d'une DMZ

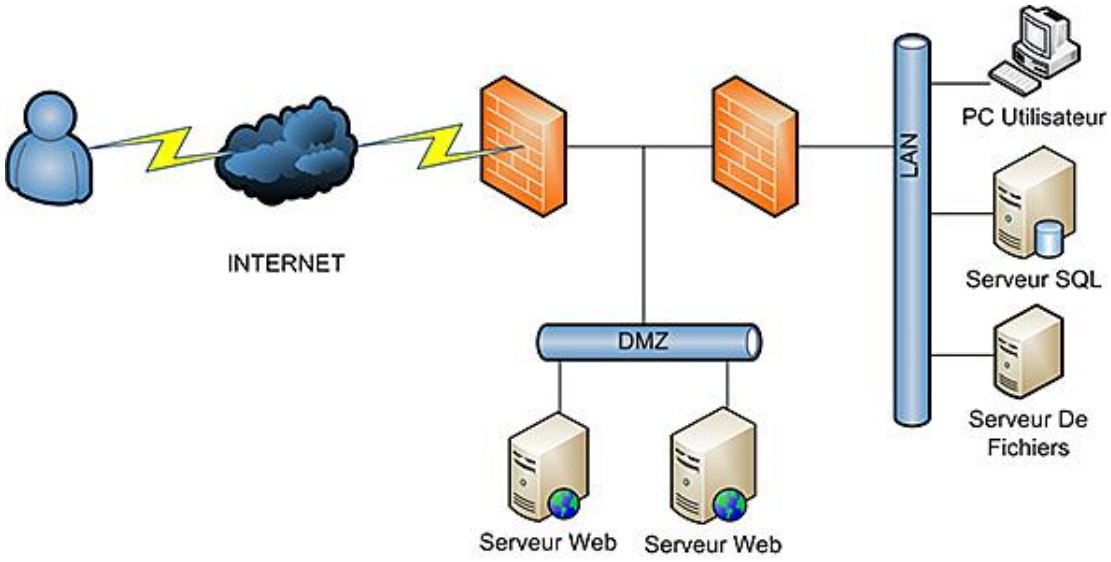
Une DMZ (*Demilitarized Zone*) ou zone Démilitarisée est un emplacement du réseau dans lequel les utilisateurs d'Internet peuvent accéder à vos serveurs sans mettre en péril la sécurité de votre réseau local. Le but de cette zone est de limiter la surface d'exposition de vos réseaux. En faisant en sorte que vos serveurs qui hébergent des applicatifs publics soient dans ce réseau périmétrique, vous ne permettez pas d'accès à votre réseau local depuis Internet. Vous renforcez donc la sécurité de votre réseau local en ne laissant pas de communication possible avec celui-ci.

Il existe deux implémentations typiques de DMZ. La première utilise un pare-feu à trois pattes ou plus (une patte correspond à une interface réseau).

© ENI Editions - All rigths reserved



La seconde quant à elle fait appel à deux pare-feu. Dans l'idéal et en vue de sécuriser un maximum, il est recommandé d'utiliser deux modèles de pare-feu différents. En effet, si une personne malintentionnée vient à trouver une faille sur le premier, le travail est déjà quasiment accompli pour arriver à percer le second.



Il ne vous reste ensuite plus qu'à gérer les flux entre Internet et DMZ, et entre la DMZ et le LAN. En effet, si vos serveurs Web font appel à des ressources du réseau, ils auront besoin d'un accès à celui-ci. Il suffit donc d'autoriser les serveurs de la DMZ à communiquer avec le LAN pour les protocoles requis. Au plus vous restreindrez les accès et au mieux seront sécurisés à la fois votre DMZ et votre réseau local.

Côté serveur, Windows 2008 Server configure automatiquement les exceptions de son Firewall. En ayant rajouté le rôle de serveur IIS, celui-ci a donc automatiquement autorisé les flux HTTP et HTTPS. Il ne vous reste alors plus qu'à gérer les ouvertures sur les équipements de pare-feu.

© ENI Editions - All rigths reserved

Monter un site Intranet

S'il n'est pas difficile de créer un site Web basique grâce à IIS, ceux d'entre vous qui ne sont pas initiés aux langages de développement Web auront du mal à satisfaire les besoins des utilisateurs pour le contenu.

Microsoft fournit gratuitement un CMS (*Content Management System*) pour répondre à ces besoins. Ce type de logiciel offre un environnement Web collaboratif dynamique qui facilite l'implémentation par des modèles pré-configurés. Il s'agit de Windows SharePoint Services. Actuellement disponible en version 3.0 avec Service Pack 1, il peut s'installer sur Windows 2003 ainsi que sur Windows Server 2008.

Pour télécharger Windows SharePoint Services 3.0 avec SP1 :

http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=EF93E453-75F1-45DF-8C6F-4565E8549C2A&displaylang=en

WSS (*Windows SharePoint Services*) offre un espace de travail unique pour organiser les documents, programmer des réunions ou encore participer à des discussions.

Sa facilité de déploiement et de personnalisation permet aux utilisateurs une gestion des documents souple et rapide.

WSS contient de base plusieurs modèles de sites applicatifs qui vous aideront dans sa mise en place. On retrouve ainsi deux grandes catégories : les modèles de collaboration et ceux de réunions.

En collaboration, vous avez accès à :

- **Site d'équipe** : correspond au modèle de base. Il propose une bibliothèque de documents, des annonces, des éléments de calendrier, des tâches et des discussions.
- **Site vide** : seule la structure est présente à vous d'ajouter les composants voulus.
- **Espace de travail du document** : il s'agit d'une bibliothèque de documents permettant à plusieurs de travailler sur un même fichier. Les fonctionnalités de gestion de version de SharePoint permettent un suivi des modifications. Une liste des tâches est associée de façon à répartir le travail entre plusieurs collaborateurs.
- **Site Wiki** : espace de partage d'idées, de définitions. Il peut être utilisé pour gérer une base de connaissances sur votre intranet.
- **Blog** : ni plus ni moins qu'un blog qui peut être alimenté en quelques clics par chaque utilisateur.

En réunions, vous avez accès à :

- **Réunion de base** : planification, organisation, compte rendu, gestion de l'ordre du jour et des participants.
- **Réunion vide** : possède uniquement la structure. La personnalisation est à réaliser en fonctions de vos besoins.
- **Réunion pour prise de décision** : suivi de l'état et la prise de décisions. Il propose une liste de création de tâches et de stockage de documents.
- **Réunion informelle** : planification d'événements informels, suivi des événements, des participants et des images liées.
- **Réunion multipage** : planification, organisation et collecte des résultats d'une réunion.

Des modèles d'applications sont disponibles gratuitement à l'adresse : http://technet.microsoft.com/fr-fr/windowsserver/sharepoint/bb407286(en-us).aspx

---

À l'heure où ce livre est écrit, il en existe une quarantaine disponibles en anglais et environ vingt en français. Ces modèles vont de la base de connaissances, à la gestion de demandes d'absence ou encore la gestion d'un stock.

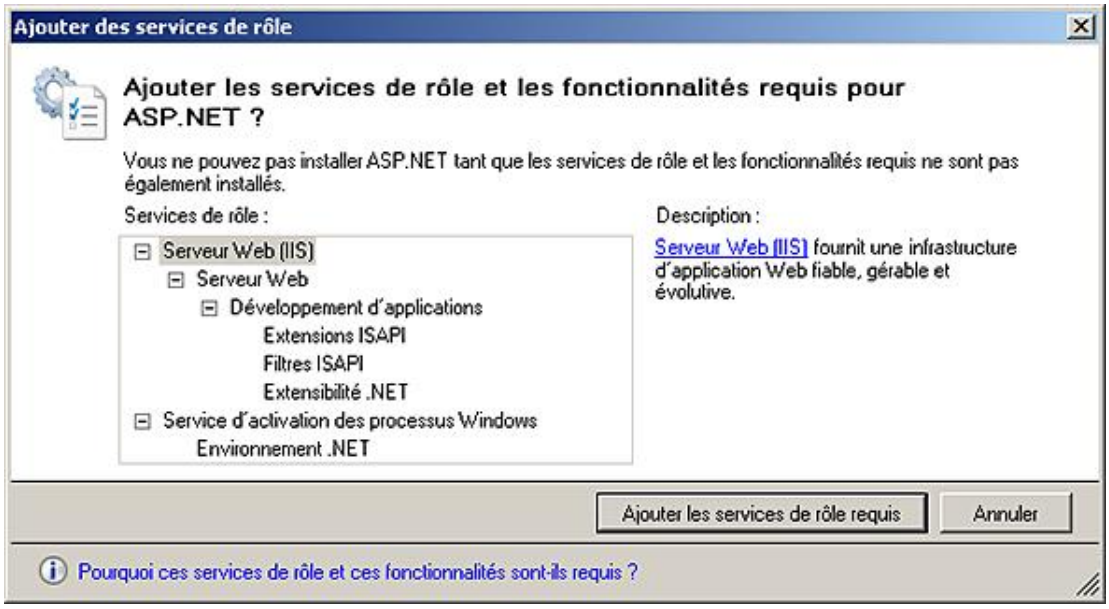
Vous allez maintenant procéder à l'installation de WSS sur votre serveur 2008.

© ENI Editions - All rigths reserved

Pré-requis : avoir téléchargé WSS avec le lien mentionné plus haut dans cette page et avoir installé le rôle de serveur IIS par défaut.

Voici les étapes pour installer les derniers pré-requis ainsi que WSS :

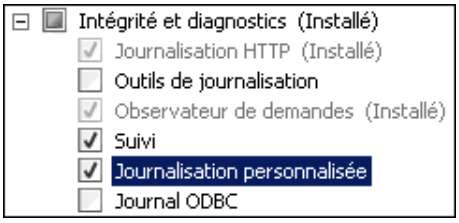
- Ouvrez votre console **Gestionnaire de serveur**.
- Dans **Rôles**, naviguez jusqu'à la section **Serveur Web (IIS)** et cliquez sur **Ajouter des services de rôle**.
- Dans la section **Développement d'applications**, cochez la case **ASP.NET**, la fenêtre suivante apparaît :


Ajouter des services de rôle
Ajouter les services de rôle et les fonctionnalités requis pour ASP.NET ?
Vous ne pouvez pas installer ASP.NET tant que les services de rôle et les fonctionnalités requis ne sont pas également installés.
Services de rôle :
Serveur Web (IIS)
Serveur Web
Développement d'applications
Extensions ISAPI
Filtres ISAPI
Extensibilité .NET
Service d'activation des processus Windows
Environnement .NET
Description :
Serveur Web (IIS) fournit une infrastructure d'application Web fiable, gérable et évolutive.
Ajouter les services de rôle requis
Annuler
Pourquoi ces services de rôle et ces fonctionnalités sont-ils requis ?

- Cliquez sur **Ajouter les services de rôle requis**.

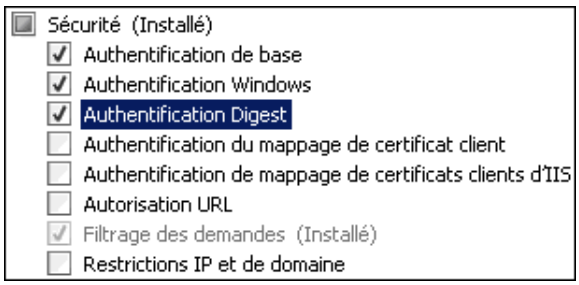
  Les cases **Extensibilité.NET** ; **Extensions ISAPI** et **Filtres ISAPI** seront automatiquement cochées.

- Dans la section **Intégrité et diagnostics**, cochez les cases **Suivi** et **Journalisation personnalisée**.



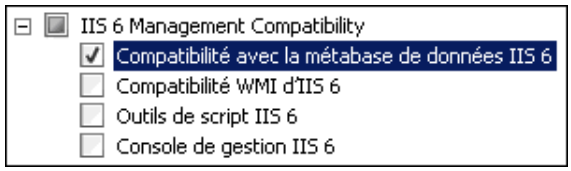
- Dans la section **Sécurité**, cochez les cases **Authentification de base**, **Authentification Windows**, **Authentification Digest**.

© ENI Editions - All rigths reserved



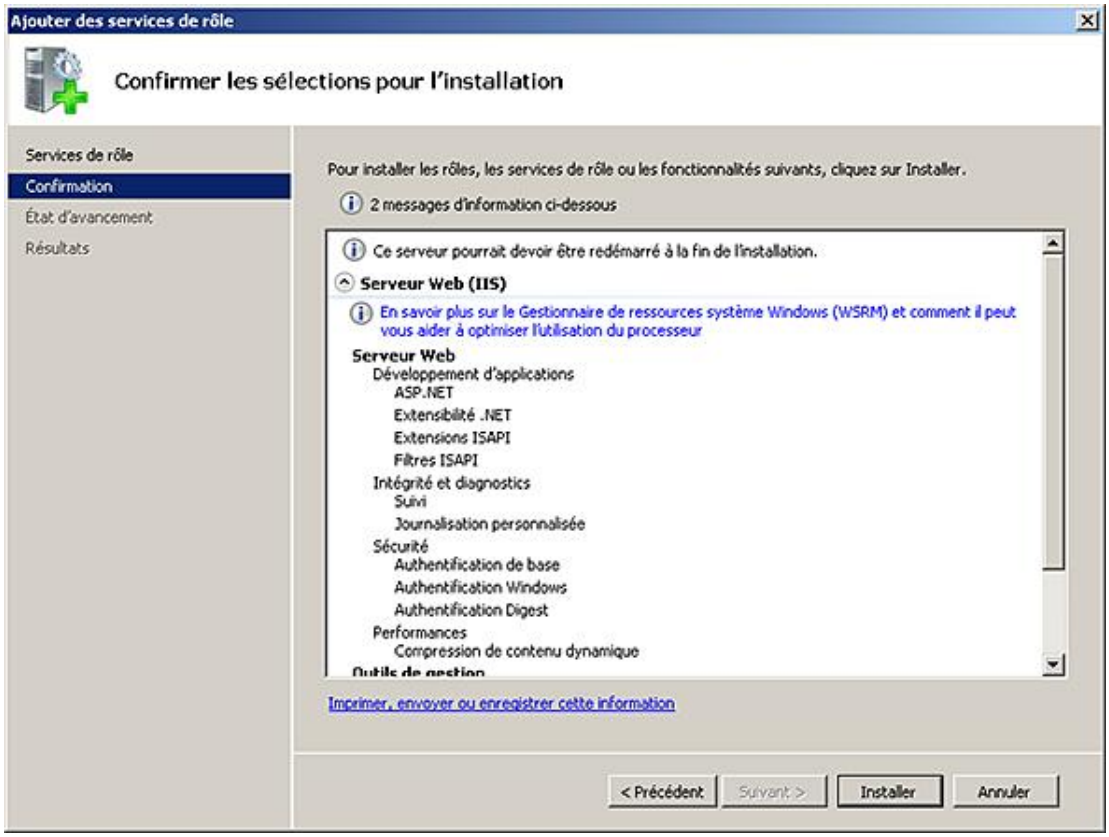
- Dans la section **Performances**, cochez la case **Compression de contenu dynamique**.

- Dans la section **IIS6 Management Compatibility**, cochez la case **Compatibilité avec la métabase de données IIS6**.


IIS 6 Management Compatibility
Compatibilité avec la métabase de données IIS 6
Compatibilité WMI d'IIS 6
Outils de script IIS 6
Console de gestion IIS 6

- Cliquez sur le bouton **Suivant**.

- Sur la page de confirmation vérifiez que vous avez sélectionné les bonnes fonctionnalités puis cliquez sur **Installer**.



- Sur la page de **Résultats**, vérifiez que l'installation s'est correctement déroulée puis cliquez sur **Fermer**.

© ENI Editions - All rigths reserved

- Retournez dans votre console **Gestionnaire de serveur** et cliquez sur **Ajouter des fonctionnalités**.
- Cochez la case **Fonctionnalités .NET Framework 3.0** puis cliquez sur **Suivant**
- Cliquez ensuite sur **Installer**.
- Sur la page de **Résultats**, vérifiez que l'installation s'est correctement déroulée puis cliquez sur **Fermer**.
- Lancez l'exécutable d'installation **Sharepoint.exe** préalablement téléchargé.
- Sur la page de licence, cochez la case **J'accepte les termes de ce contrat** puis cliquez sur **Continuer**.
- Cliquez sur la case **De base**.

L'installation de base installe également une version allégée de SQL sur le serveur. Dans le cas où vous voudriez utiliser un serveur SQL distant, cliquez sur **Avancé**. La configuration des bases SQL se fera à la fin de l'installation de la partie Web grâce à l'assistant de configuration.

- Une fois l'installation terminée, cliquez sur **Fermer** pour lancer l'assistant de configuration.
- Cliquez sur **Suivant** puis dans la fenêtre d'avertissement cliquez sur **Oui** (attention certains services dont IIS vont être redémarrés).
- Sur la page de résultats, cliquez sur **Fermer**.

La page d'accueil du site SharePoint se lance :

À partir de cette page, vous pouvez facilement personnaliser les éléments apparents comme le logo ou encore le titre de la page. La plupart des paramètres sont accessibles depuis le bouton **Actions du site** situé en haut à droite. Aucune intervention sur le code source de la page n'est nécessaire pour modifier celle-ci !

Pour accéder à la configuration du site, il vous faut passer par les outils d'administration. Là se trouve un raccourci vers la page d'**Administration centrale de SharePoint**. Cette page permet par exemple de spécifier un serveur mail entrant et sortant pour les notifications, la configuration de la fonction de recherche, etc.

© ENI Editions - All rigths reserved

Pour vous aider dans la prise en main du produit voici un lien pointant vers le TechNet de Microsoft : http://technet.microsoft.com/en-us/windowsserver/sharepoint/default.aspx

WSS vous offre donc la possibilité de déployer facilement, et à moindre coût, un environnement collaboratif. La création et la personnalisation sont simplifiées. Les accès peuvent être configurés de façon très précise de sorte à sécuriser les informations de votre Intranet. Vous avez un suivi des documents et de leur modification et vous renforcez ainsi le travail en équipe.

Si certaines fonctionnalités venaient à manquer, sachez que Microsoft propose également une solution payante plus complète appelée MOSS (*Microsoft Office SharePoint Server 2007*). Les possibilités sont par contre plus étendues. À titre d'exemple, il permet de créer des sites individuels pour chaque employé (appelé **My site**), la gestion de flux RSS, des modèles de site portail, etc. MOSS s'intègre également à la suite Office 2007. Il est du coup possible de lancer ou participer à un Workflow directement depuis les programmes de la suite Office 2007 (Word, Excel, etc.). Il offre également la possibilité de s'interfacer avec des produits tiers comme SAP ou encore Siebel et les modèles de site sont plus nombreux et répondent aux besoins des grandes organisations.

Vous pouvez trouver une comparaison entre les différentes versions de SharePoint à l'adresse suivante : http://office.microsoft.com/en-us/sharepointtechnology/FX101758691033.aspx

Vous venez de voir dans ce chapitre que pour gérer des sites Internet et/ou Intranet vous devez utiliser le rôle de Serveur Web (IIS).

Dans sa version 7, IIS offre de nombreux rôles de services liés à la sécurité, la performance, le diagnostic ou encore la rétrocompatibilité.

L'architecture de IIS7 a été repensée pour renforcer la sécurité et apporter une modularité non présente dans les versions précédentes.

Les outils d'administration ont été étendus. Vous pouvez utiliser comme avant l'interface graphique mais aussi les outils en ligne de commande comme AppCMD et Powershell pour automatiser vos tâches.

Windows Sharepoint Services avec son site Web par défaut vous permet de publier facilement un site Web sur votre intranet. Ce site peut alors être personnalisé par les utilisateurs sans qu'ils aient la moindre compétence en terme de développement.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre est consacré à la sécurisation de Windows Server 2008. La sécurité est au cœur de cet OS, pour laquelle la mise en œuvre la plus flagrante est l'installation dite « minimum », dont le nom anglais «Core » est très répandu pour la nommer. À travers ce chapitre, vous allez découvrir comment gérer cette « version » si particulière, et si utile en environnement hostile.

© ENI Editions - All rigths reserved

Principes du serveur Core

Cette section présente les principales caractéristiques du serveur Core, les domaines de prédilection pour lesquels il a été prévu, ainsi que ceux pour lesquels il n'est pas possible de l'utiliser.

1. Restrictions liées à une installation Core

L'intérêt d'une installation Core est de réduire la surface d'attaque a un impact sur les rôles pouvant être installés sur un serveur Core, notamment tous les services utilisant un Framework Microsoft .Net, absent de ce type d'installation. Les rôles suivants peuvent être installés :

- Contrôleur de domaine (typiquement un RODC) ;
- Annuaire ADAM ;
- Serveur DHCP et DNS ;
- Serveur de fichiers ;
- Hyper-V (domaine de prédilection) ;
- Serveur d'impressions ;
- Serveur Web IIS (attention, pas de .Net).

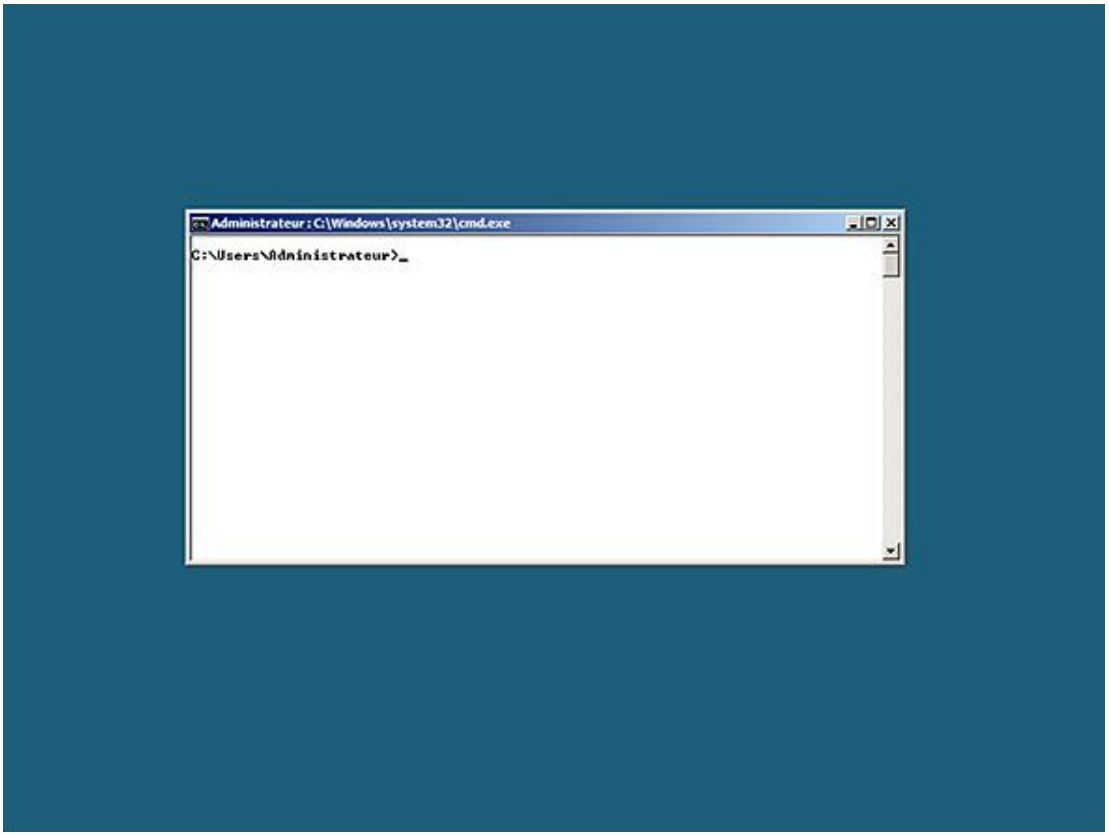
La sortie de Windows Server 2008 R2 enrichira cette liste, notamment par l'ajout du Framework .Net ainsi que des nouvelles possibilités liées à cet ajout.

2. Installation minimale

L'installation Core est succincte, et cela se voit dès l'installation ! Seulement 6 minutes et 30 secondes ont été nécessaires pour passer de l'insertion du DVD d'installation au prompt d'authentification, et ce même sans automatiser l'installation.

À ce stade, rien n'indique qu'il s'agit d'une installation minimale. Ce n'est qu'une fois authentifié que la différence est « frappante » :

© ENI Editions - All rigths reserved



Il ne s'agit pas d'une capture d'écran partielle, mais bien de l'écran entier. Explorer n'est pas dissimulé quelque part, le binaire est bel et bien absent du disque dur ! L'objectif est de réduire au maximum les composants et ressources, ce qui est à la fois pertinent pour la sécurité et les machines virtuelles.

Du point de vue de la sécurité, moins d'éléments sont installés, exécutés ou accessibles, plus le niveau de sécurité augmente. Par exemple, puisqu'il n'y a pas *Explorer.exe*, toute faille de sécurité l'affectant n'aura aucun impact sur un serveur Core. Au delà du fait que la faille ne fonctionne pas, il n'est même pas nécessaire d'installer le hotfix qui corrigera la faille plus tard. Si une version Core de Windows Server 2000 avait existé, elle aurait réduit d'environ 60 % le nombre des mises à jour à installer, et d'environ 40 % sur Windows Server 2003. L'empreinte du système d'exploitation est également fortement réduite :

- Au démarrage, avec juste une session ouverte, 215 Mo de mémoire sont utilisés, contre plus de 400 Mo sur une installation complète.

- 1,3 Go d'espace disque est nécessaire, contre presque 11 Go sur une installation complète.

© ENI Editions - All rigths reserved

Configurer localement un Serveur Core

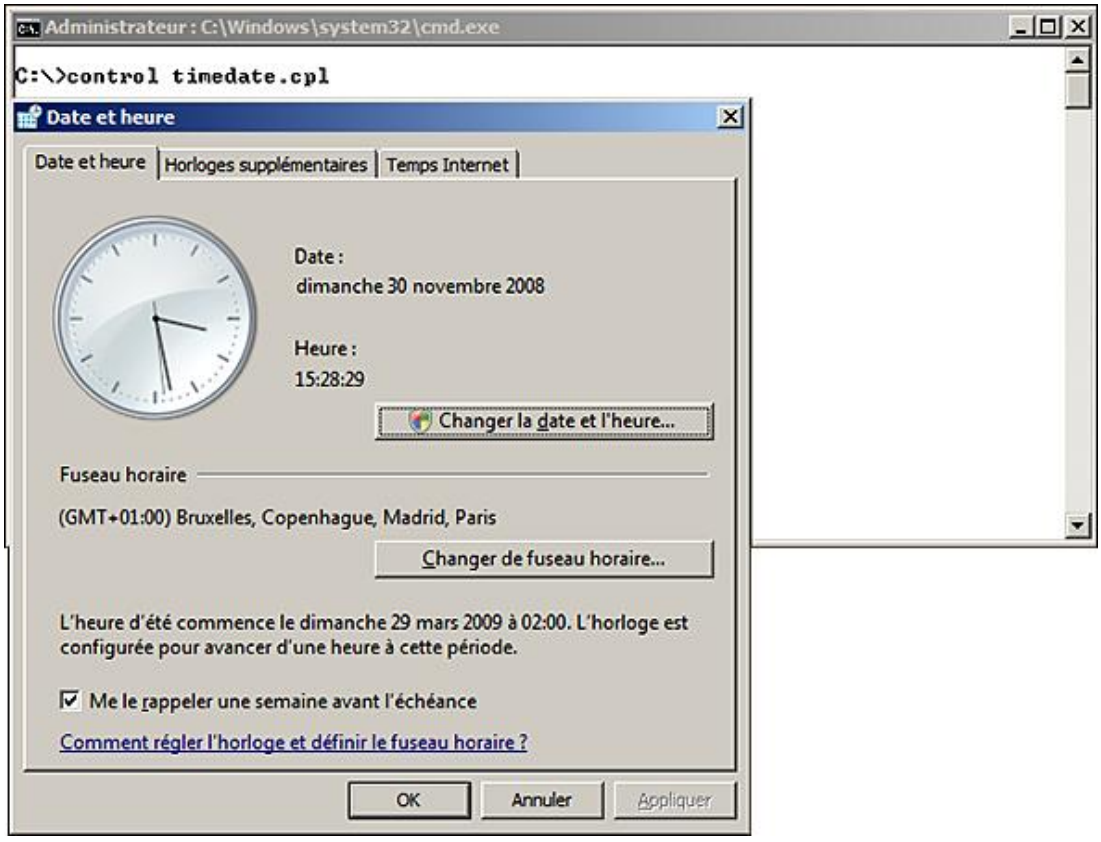
L'absence des consoles d'administrations même de PowerShell n'incite pas à administrer localement un serveur Core, ce qui est une partie de l'objectif. Une fois le minimum de configuration effectué, il suffit de s'y connecter depuis un hôte distant qui lui a les consoles d'administration pour s'affranchir de ces contraintes. Cette section couvre la configuration initiale pour permettre une administration décentralisée.

1. Configurer le temps

Certaines actions évidentes sur un serveur classique peuvent paraître déroutantes dans cette installation épurée. Une des premières actions à effectuer sur un serveur est de configurer la date et l'heure. Même si celui-ci va rejoindre un domaine, il doit avoir par défaut moins de 5 minutes de décalage avec l'heure du domaine pour que Kerberos puisse fonctionner et ainsi permettre la jonction du domaine.

Plusieurs solutions existent (les commandes `time` et `date` sont toujours présentes), mais voici comment récupérer un peu de graphique sous serveur Core :

- Depuis la ligne de commande, exécutez `control timedate.cpl` :


Administrateur : C:\Windows\system32\cmd.exe
C:\>control timedate.cpl
Date et heure
Date et heure
Horloges supplémentaires
Temps Internet
Date :
dimanche 30 novembre 2008
Heure :
15:28:29
Changer la date et l'heure...
Fuseau horaire
(GMT+01:00) Bruxelles, Copenhague, Madrid, Paris
Changer de fuseau horaire...
L'heure d'été commence le dimanche 29 mars 2009 à 02:00. L'horloge est configurée pour avancer d'une heure à cette période.
Me le rappeler une semaine avant l'échéance
Comment régler l'horloge et définir le fuseau horaire ?
OK
Annuler
Appliquer

2. Paramètres régionaux

Si vous souhaitez modifier les paramètres régionaux, vous pouvez utiliser la commande `control intl.cpl`.

3. Résolution de l'écran

La seule solution pour changer la résolution de l'écran est de passer par la base de registre. Pour cela, appelez l'éditeur `regedit` depuis la ligne de commande ouverte à l'écran.

- Naviguez dans l'arborescence jusqu'à cette racine :

© ENI Editions - All rigths reserved

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Video.

Un identifiant aléatoire a été affecté à votre carte graphique. Vous pouvez déterminer lequel y correspond en regardant la sous-clé **Device Description** à l'intérieur.

Quatre clés permettent de gérer la résolution, le nombre de couleurs et le taux de rafraîchissement :

- **DefaultSettings.XResolution** : nombre de pixels sur l'axe horizontal.
- **DefaultSettings.YResolution** : nombre de pixels sur l'axe vertical.
- **DefaultSettings.BitsPerPel** : nombre de couleurs (32 bits par défaut).
- **DefaultSettings.VRefresh** : taux de rafraîchissement de l'écran.

4. Économiseur d'écran

L'économiseur d'écran peut être modifié aussi en ligne de commande. Pour cela, appelez l'éditeur `regedit` depuis la ligne de commande ouverte à l'écran.

- Naviguez dans l'arborescence jusqu'à cette racine : **HKEY_CURRENT_USER\Control Panel\Desktop**.

Trois clés permettent de gérer le nom de l'économiseur d'écran, le verrouillage de la session suite au lancement de l'économiseur d'écran et le temps d'attente avant de le lancer :

- **ScreenSaveActive** : permet d'activer ou désactiver l'économiseur d'écran de façon globale. Il peut prendre les valeurs **1** (actif) ou **0** (inactif).
- **SCRNSAVE.EXE** : spécifie l'économiseur d'écran à exécuter. Le paramètre par défaut est **C:\Windows\system32\logon.scr**. L'économiseur d'écran **scrsave.scr** est disponible sur le serveur, ce qui évite une consommation processeur inutile, notamment en environnement virtuel.
- **ScreenSaverIsSecure** : permet d'activer ou non le verrouillage de la session à l'exécution de l'économiseur d'écran. La valeur par défaut est **1**, ce qui rend active cette protection.
- **ScreenSaveTimeOut** : nombre de secondes avant le déclenchement de l'économiseur d'écran. Par défaut, la valeur est 600 secondes.

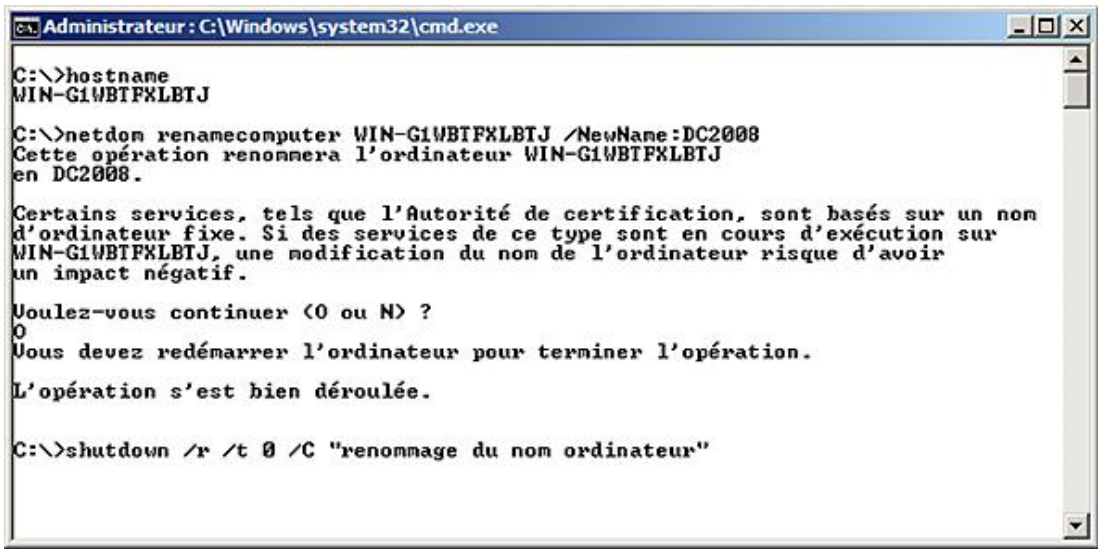
Dans le cadre d'un domaine Active Directory, ces paramètres peuvent être gérés par stratégies de groupe de façon centrale.

5. Nom du serveur

Par défaut, un nom de machine aléatoire est donné au serveur, toujours préfixé par **WIN-**.

- Pour connaître le nom actuel, exécutez la commande suivante depuis la ligne de commandes : `hostname`
- Pour changer le nom du serveur, exécutez la commande suivante depuis la ligne de commandes : `netdom renamecomputer <nomdevotreserveur> /NewName:DC2008`
- Il faut redémarrer pour prendre en compte ce changement : `shutdown /r /t 0 /C "renommage du nom ordinateur"`

© ENI Editions - All rigths reserved


Administrateur : C:\Windows\system32\cmd.exe
C:\>hostname
WIN-G1WBTFXLBTJ
C:\>netdom renamecomputer WIN-G1WBTFXLBTJ /NewName:DC2008
Cette opération renommera l'ordinateur WIN-G1WBTFXLBTJ
en DC2008.
Certains services, tels que l'Autorité de certification, sont basés sur un nom
d'ordinateur fixe. Si des services de ce type sont en cours d'exécution sur
WIN-G1WBTFXLBTJ, une modification du nom de l'ordinateur risque d'avoir
un impact négatif.
Voulez-vous continuer (O ou N) ?
O
Vous devez redémarrer l'ordinateur pour terminer l'opération.
L'opération s'est bien déroulée.
C:\>shutdown /r /t 0 /C "renommage du nom ordinateur"

6. Gestion des pilotes

La gestion des pilotes est possible via la ligne de commande, avec l'outil **pnputil**.

Vous pouvez lister les pilotes tiers installés en exécutant cette commande : `Pnputil -e`

Pour ajouter et installer des pilotes supplémentaires, il faut utiliser les paramètres `-a` et `-i` et préciser le dossier où les trouver : **Pnputil -a -i c:\mespilotes*.inf**

Pour obtenir la liste des pilotes actifs : `sc query type= driver`

7. Configuration réseau

Le serveur est par défaut en adressage DHCP sur toutes les interfaces. Pour passer en adressage IP statique, vous allez utiliser la commande `netsh`. Elle existe depuis Windows 2000, mais son usage n'est pas très répandu chez les administrateurs système. Chaque carte réseau a un numéro attribué, qui est utilisé par `netsh` pour déterminer la carte réseau à laquelle appliquer les changements. Pour lister les cartes réseaux et voir les identifiants attribués par Windows, depuis la ligne de commande, exécutez :

```
netsh interface ipv4 show interfaces
```

- Par exemple, si vous souhaitez configurer la carte réseau ayant l'identifiant 2 en adressage IP statique, exécutez :

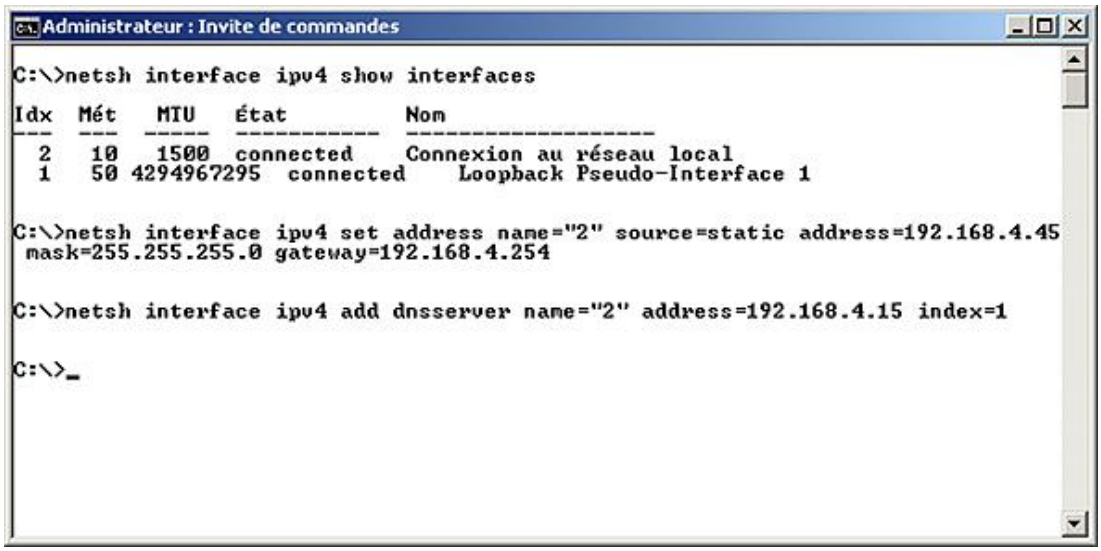
```
netsh interface ipv4 set address name="2" source=static
address=192.168.4.45 mask=255.255.255.0 gateway=192.168.4.254
```

- Pour configurer l'adresse 192.168.4.15 comme serveurs DNS primaire, exécutez la commande :

```
netsh interface ipv4 add dnsserver name="2"
address=192.168.4.15 index=1
```

Vous devriez avoir un résultat équivalent à celui-ci :

© ENI Editions - All rigths reserved


Administrateur : Invite de commandes
C:\>netsh interface ipv4 show interfaces
Idx Mét MTU État Nom
2 10 1500 connected Connexion au réseau local
1 50 4294967295 connected Loopback Pseudo-Interface 1
C:\>netsh interface ipv4 set address name="2" source=static address=192.168.4.45 mask=255.255.255.0 gateway=192.168.4.254
C:\>netsh interface ipv4 add dnsserver name="2" address=192.168.4.15 index=1
C:\>_

La commande `netsh` accepte l'argument `store`, qui permet d'indiquer si la configuration doit persister après le prochain redémarrage du serveur, ce qui est le cas si le paramètre est omis. Si vous ne souhaitez pas conserver le paramétrage effectué après le redémarrage, vous pouvez ajouter l'argument `store=active`. Si vous souhaitez expliciter le fait que le paramétrage doit être persistant, vous pouvez utiliser l'argument `store=persistent`.

Pour configurer le suffixe DNS par défaut, il faut modifier la base de registre. Pour ce faire, depuis la ligne de commande, exécutez :

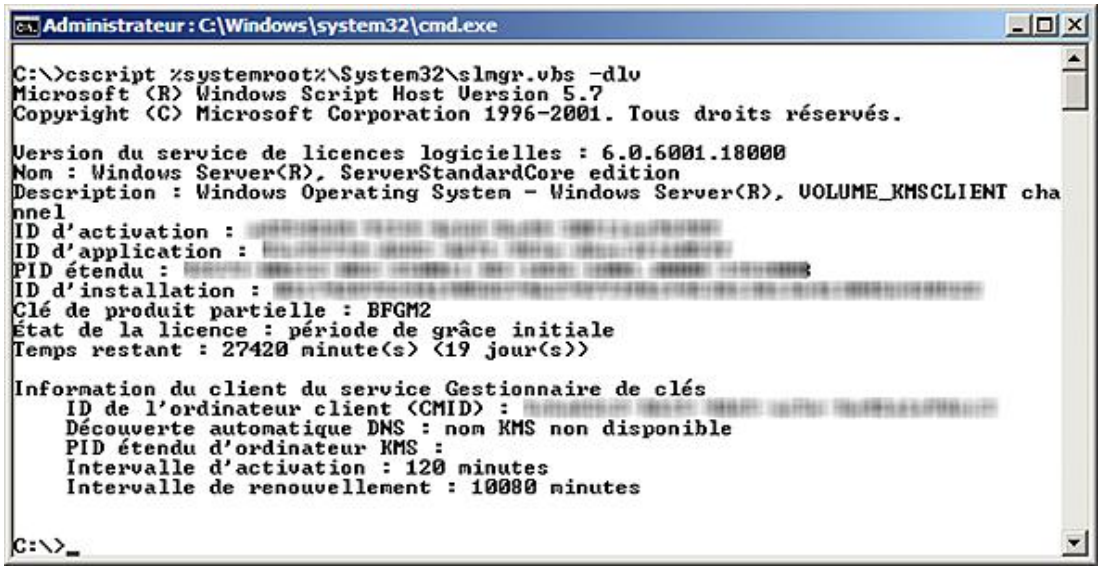
```
reg add HKLM\SYSTEM\ CurrentControlSet\
Services\Tcpip\Parameters /v "NV Domain" /d "bigfirm.com" /f
```

8. Activation de Windows

La gestion de l'activation de la licence Windows est gérable en ligne de commande. Le script VB `slmgr.vbs` est installé avec Windows dans %systemroot%\System32 à cet effet. Pour rappel, contrairement aux versions précédentes de Windows, l'activation est obligatoire, même avec une licence en volume. Ce script fonctionne aussi avec KMS (*Key Management Service*).

Pour vérifier l'état d'activation actuel, exécutez la commande :

```
cscript %systemroot%\System32\slmr.vbs -dlv
```


Administrateur : C:\Windows\system32\cmd.exe
C:\>cscript %systemroot%\System32\slmgr.vbs -dlv
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
Version du service de licences logicielles : 6.0.6001.18000
Nom : Windows Server(R), ServerStandardCore edition
Description : Windows Operating System - Windows Server(R), VOLUME_KMSCLIENT channel
ID d'activation :
ID d'application :
PID étendu :
ID d'installation :
Clé de produit partielle : BFGM2
État de la licence : période de grâce initiale
Temps restant : 27420 minute(s) (19 jour(s))
Information du client du service Gestionnaire de clés
ID de l'ordinateur client (CMID) :
Découverte automatique DNS : nom KMS non disponible
PID étendu d'ordinateur KMS :
Intervalle d'activation : 120 minutes
Intervalle de renouvellement : 10080 minutes
C:\>_

Dans cet exemple, la licence expire dans 19 jours.

Si vous souhaitez juste connaître la date à laquelle la licence expire, exécutez le script avec le paramètre `-xpr`.

© ENI Editions - All rigths reserved

Administrateur : C:\Windows\system32\cmd.exe
C:\>cscript %systemroot%\System32\slmgr.vbs -xpr
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
La période de grâce initiale se termine le 29/01/2009 13:53:41
C:\>_

Par défaut, le service KMS est automatiquement trouvé sur votre domaine Active Directory à travers la requête DNS suivante : `_vlmcs._tcp.masociete.local`.

Si cette entrée DNS existe, le serveur essayera de s'y connecter sur le port TCP 1688. Vous pouvez aussi indiquer manuellement le nom du serveur KMS avec le paramètre `-skms`.

Pour déclencher manuellement l'activation de Windows, exécutez la commande :

```
cscript %systemroot%\System32\slmr.vbs -ato
```

9. Gestion du rapport d'erreurs

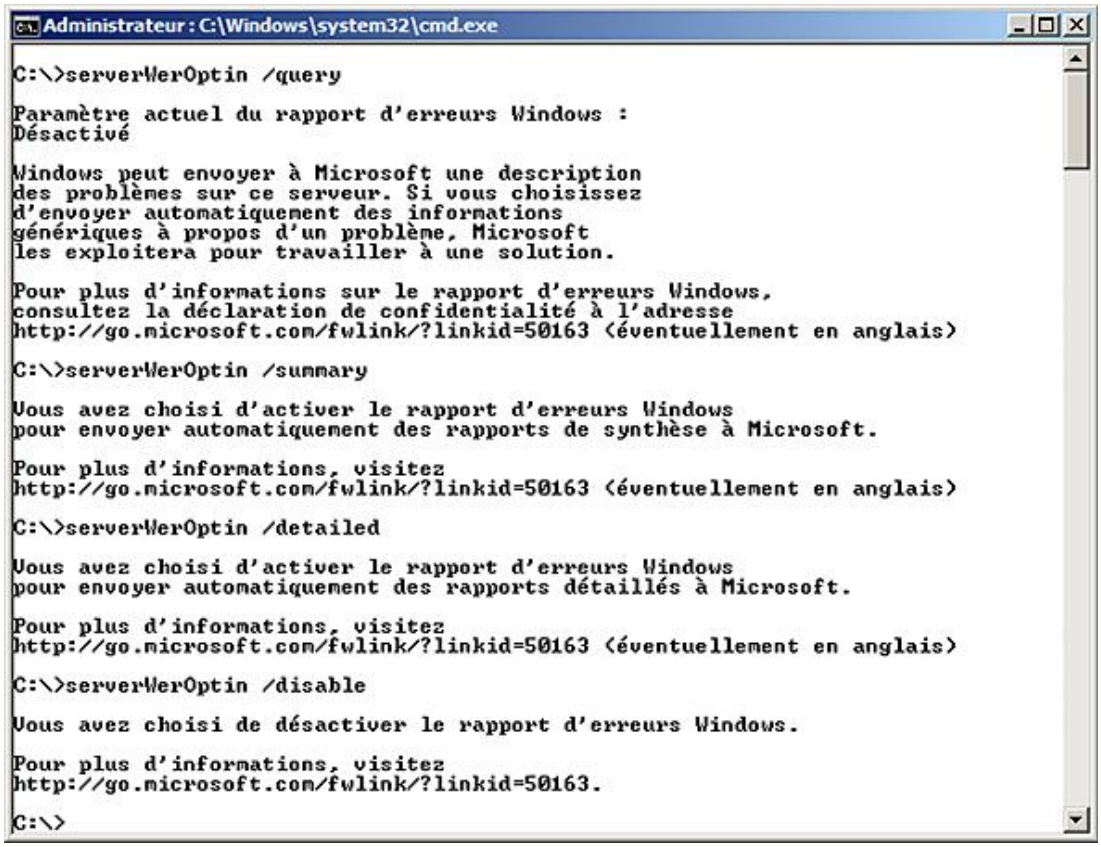
Le service de rapport d'erreurs peut être configuré depuis la ligne de commande.

Pour vérifier la configuration actuelle, exécutez la commande `serverWerOptin /query`.

Pour activer le rapport d'erreurs détaillé : `serverWerOptin /detailed`.

Pour activer le rapport d'erreurs simple : `serverWerOptin /summary`.

Pour désactiver le rapport d'erreurs : `serverWerOptin /disable`.


Administrateur : C:\Windows\system32\cmd.exe
C:\>serverWerOptin /query
Paramètre actuel du rapport d'erreurs Windows :
Désactivé
Windows peut envoyer à Microsoft une description
des problèmes sur ce serveur. Si vous choisissez
d'envoyer automatiquement des informations
génériques à propos d'un problème, Microsoft
les exploitera pour travailler à une solution.
Pour plus d'informations sur le rapport d'erreurs Windows,
consultez la déclaration de confidentialité à l'adresse
http://go.microsoft.com/fwlink/?linkid=50163 (éventuellement en anglais)
C:\>serverWerOptin /summary
Vous avez choisi d'activer le rapport d'erreurs Windows
pour envoyer automatiquement des rapports de synthèse à Microsoft.
Pour plus d'informations, visitez
http://go.microsoft.com/fwlink/?linkid=50163 (éventuellement en anglais)
C:\>serverWerOptin /detailed
Vous avez choisi d'activer le rapport d'erreurs Windows
pour envoyer automatiquement des rapports détaillés à Microsoft.
Pour plus d'informations, visitez
http://go.microsoft.com/fwlink/?linkid=50163 (éventuellement en anglais)
C:\>serverWerOptin /disable
Vous avez choisi de désactiver le rapport d'erreurs Windows.
Pour plus d'informations, visitez
http://go.microsoft.com/fwlink/?linkid=50163.
C:\>

10. Joindre un domaine

La commande `netdom` permet aussi de joindre un domaine Active Directory existant. Depuis la ligne de commande, exécutez :

© ENI Editions - All rigths reserved

```
netdom join <nomdemonserveur> /domain:<monDomainAD>
userd:<CompteADayantLesDroits> /passwordd:*
```

Le symbole * indique que le mot de passe doit être demandé ensuite, évitant qu'il ne soit écrit en clair dans la console.

La même commande permet de quitter un domaine Active Directory : `netdom remove`.

11. Gérer les journaux d'évènements

Bien que la console **Observateurs d'évènements** permette de voir les journaux d'un serveur distant, vous pouvez être amené à les gérer localement depuis le serveur Core. La liste des journaux peut être affichée sur la console avec la commande : `wevtutil el`.

La fenêtre Invite de commandes n'étant pas l'idéal pour un affichage massif ni très rapide, vous pouvez restreindre la sortie en spécifiant le nombre d'évènements à afficher. Par exemple, pour n'afficher que les cinq derniers évènements : `wevtutil qe System /c:5 /f:Text`.

Il est même possible d'avoir uniquement les cinq dernières erreurs en ajoutant le paramètre `"/q:*[System[(Level=1 or Level=2)]]"`.

Le niveau 1 correspond aux évènements « critiques ».

Le niveau 2 correspond aux évènements « erreurs ».

Le niveau 3 correspond aux évènements « avertissements ».

Le niveau 4 correspond aux évènements « informations ».

Vous pouvez archiver le journal ouvert dans un fichier d'archive et ainsi commencer un nouveau journal avec la commande :

```
wevtutil cl system /bu:c:\MesArchives\syslog.evtx
```


© ENI Editions - All rigths reserved

Gestion à distance

1. Activation du bureau à distance

Comme tout Windows Server 2008, l'accès à distance n'est pas activé par défaut. Vous pouvez vérifier l'activation ou non avec la commande suivante :

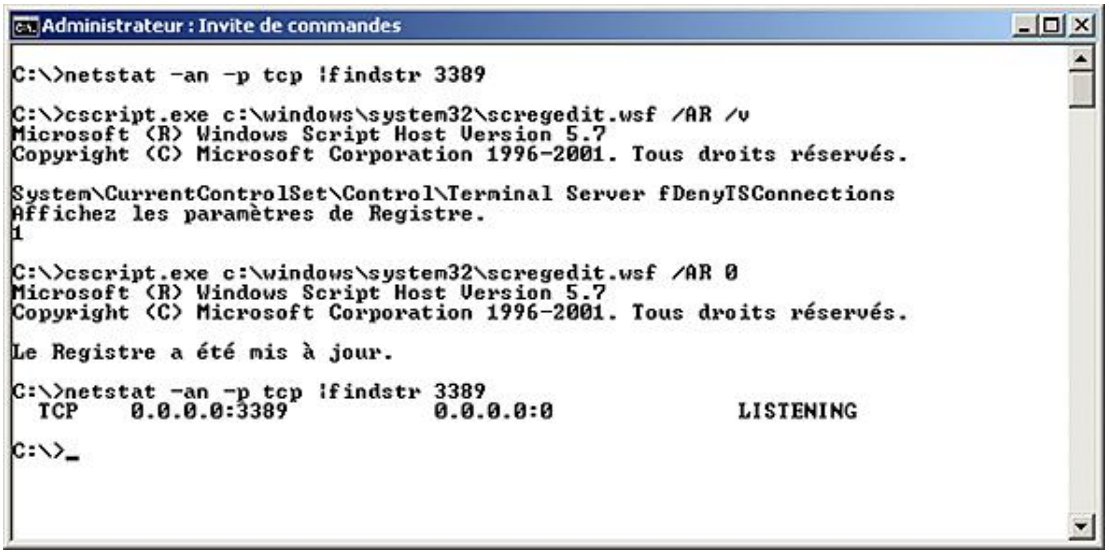
```
cscript.exe c:\windows\system32\scregedit.wsf /AR /v
```

Comme expliqué au chapitre Terminal Services - Administration à distance, la clé **fDenyTSConnections** désactive la prise de main à distance lorsqu'elle est positionnée à **1**, comme actuellement. Le même script permet de passer la clé à zéro afin d'activer les connexions :

```
cscript.exe c:\windows\system32\scregedit.wsf /AR 0
```

À ce stade, seuls les clients exécutant au moins Windows Vista ou Windows Server 2008 pourront se connecter. Pour autoriser les clients antérieurs à s'y connecter :

```
cscript.exe c:\windows\system32\scregedit.wsf /cs 0
```


Administrateur : Invite de commandes
C:\>netstat -an -p tcp |findstr 3389
C:\>cscript.exe c:\windows\system32\scregedit.wsf /AR /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
System\CurrentControlSet\Control\Terminal Server fDenyTSConnections
Affichez les paramètres de Registre.
1
C:\>cscript.exe c:\windows\system32\scregedit.wsf /AR 0
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
Le Registre a été mis à jour.
C:\>netstat -an -p tcp |findstr 3389
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
C:\>

2. Activation de WinRM

WinRM est l'implémentation par Microsoft du protocole WS-Management. L'objectif est de pouvoir communiquer entre deux systèmes à travers le système d'information, en pouvant correctement traverser les firewalls. Pour installer WinRM, exécutez cette commande depuis le prompt de commande : `WinRM quickconfig`.

Vous pouvez vérifier que winRM écoute en utilisant la commande :

```
winrm enumerate winrm/config/listener
```

Quickconfig se charge d'ajouter l'exception sur le firewall afin que le service soit accessible via le réseau.

© ENI Editions - All rigths reserved

Administrateur : C:\Windows\system32\cmd.exe
C:\>winrm quickconfig
WinRM n'est pas configuré pour la gestion à distance de cet ordinateur.
Les modifications suivantes doivent être effectuées :
Créez un écouteur WinRM sur HTTP://* pour accepter les demandes de la gestion de
s services Web sur toutes les adresses IP de cet ordinateur.
Activez l'exception de pare-feu WinRM.
Effectuer ces modifications [y/n] ? y
WinRM a été mis à jour pour la gestion à distance.
Écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion des se
rvices Web sur toutes les adresses IP de cet ordinateur.
Exception de pare-feu WinRM activée.
C:\>winrm enumerate winrm/config/listener
Listener
Address = *
Transport = HTTP
Port = 80
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 192.168.4.45, ::1, fe80::5efe:192.168.4.45%3, fe80:
:ffff:ffff:fffe%4, fe80::5df0:d43b:a56e:ae72%2
C:\>

Par défaut, WinRM utilise le protocole HTTP. Il est possible d'utiliser HTTPS, à condition d'avoir déjà installé un certificat valide (non expiré, non auto-signé…). Pour cela, il suffit de spécifier le transport HTTPS : `WinRM quickconfig -transport:https`. Si vous souhaitez utiliser WinRM pour accéder à un serveur qui n'est pas dans votre domaine Active Directory, vous devez soit utiliser un certificat SSL, soit utiliser la liste des ordinateurs approuvés. Cette liste étant côté client, vous pourrez potentiellement la gérer par stratégie de groupe, facilitant ainsi les ajouts et suppressions de serveurs à cette liste.

Si vous souhaitez gérer directement en local cette liste, vous pouvez utiliser la commande suivante pour ajouter des serveurs :

```
winrm set winrm/config/client @{TrustedHosts="<maliste>"}
```

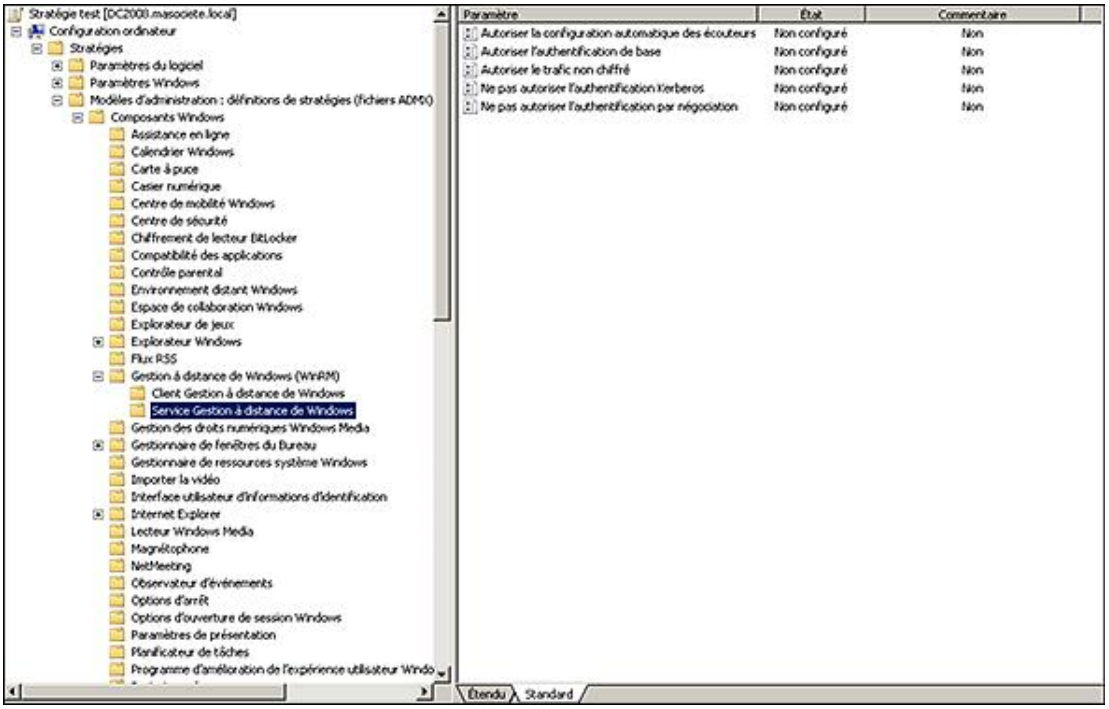
Il faudra remplacer *maliste* par un ou plusieurs éléments séparés par des virgules. Les adresses IP et noms DNS peuvent être utilisés.

Pour obtenir la liste actuelle des hôtes approuvés :

```
winrm get winrm/config/client
```

Si vos serveurs sont dans un domaine Active Directory, vous pouvez gérer WinRM depuis les stratégies de groupe :

© ENI Editions - All rigths reserved



Il serait tout à fait regrettable d'évoquer ce protocole sans expliciter par l'exemple ses capacités. Voici donc quelques possibilités avec WinRM.

- Afficher le résultat de la commande `ipconfig /all` d'un hôte distant :

```
winrs -r:NomDuServeur ipconfig /all
```

- Spécifier un compte utilisateur et un mot de passe (le mot de passe est demandé ensuite) :

```
winrs -r:NomDuServeur -u monautrecompte ipconfig /all
```

- Faire une requête WMI :

```
winrm get wmicimv2/win32_service?name=W32Time -r :NomDuServeur
```

WinRM est aussi disponible pour les versions antérieures de Windows (XP, 2003) comme composant supplémentaire. Il est en téléchargement à cette adresse :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=845289ca-16cc-4c73-8934-dd46b5ed1d33

© ENI Editions - All rigths reserved

Sécuriser le Serveur Core

1. Gestion du pare-feu

Comme sa grande sœur, l'édition minimale a le firewall Windows actif par défaut. Cela est très visible, car le serveur ne répond pas au fameux ping, alors que pourtant l'adresse mac correspondante à l'IP est visible depuis la commande `arp -a`. La gestion des règles du firewall peut s'avérer complexe, aussi il est plus aisé de les gérer à distance. Cela peut se faire via les stratégies de groupes, mais aussi en utilisant la console adéquat de manière déportée. Avant de pouvoir faire cela, il faut autoriser la gestion des règles firewall à distance sur le serveur, en exécutant la commande suivante :

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

La console **Pare-feu Windows avec fonctions avancées de sécurité** ne permet pas directement de choisir un ordinateur distant. Pour se faire, il faut d'abord lancer le gestionnaire de console, **mmc**, puis ajouter la console **Pare-feu Windows avec fonctions avancées de sécurité**, et à ce moment là vous aurez la possibilité de choisir l'ordinateur cible. Vous trouverez davantage d'informations sur la configuration du pare-feu en mode graphique dans le chapitre Sécuriser votre architecture.

Les autres mmc peuvent être autorisées sur le pare-feu afin de pouvoir être utilisées à distance. Voici une liste d'éléments enfichables avec leur nom correspondant dans les règles :

- Services : Gestion à distance des services ;
- Planificateur de tâches : Gestion à distance des tâches planifiées ;
- Observateur d'événements : Gestion à distance des journaux des événements ;
- Moniteur de fiabilité et de performances : Journaux et alertes de performance ;
- Gestion du partage et du stockage : Partage de fichiers et d'imprimantes.

```
Netsh advfirewall firewall set rule group= " nom_des_regles"
new enable=yes
```

Pour gérer à distance IPSec, il faut tout d'abord activer sa gestion à distance:

```
cscript \windows\System32\scregedit.wsf /im 1
```

Pour que la gestion des volumes à distance fonctionne, il faut démarrer au préalable le service disque virtuel : `net start vds`.

2. Gestion automatique des mises à jour

L'activation ou la désactivation des mises à jour automatiques peut être gérée en local. Si le serveur joint un domaine Active Directory, vous devriez vraiment gérer le paramétrage via les stratégies de groupes.

- Pour savoir si les mises à jour sont activées :

```
cscript C:\Windows\System32\Scregedit.wsf /au /v
```

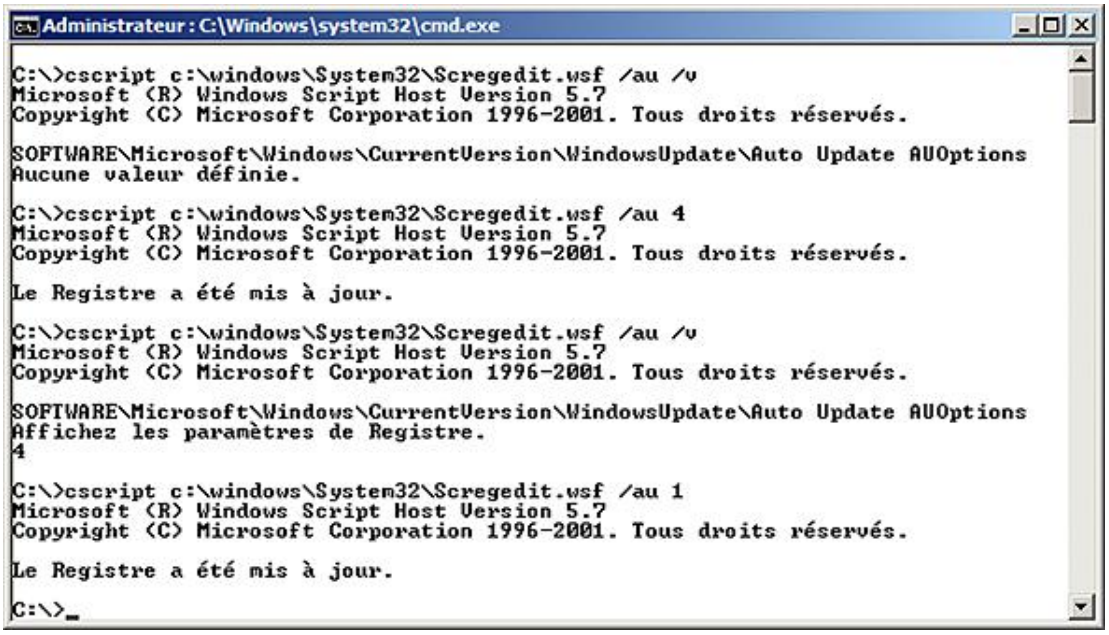
- Pour activer les mises à jour :

```
cscript C:\Windows\System32\Scregedit.wsf /au 4
```

- Pour désactiver les mises à jour :

© ENI Editions - All rigths reserved

```
cscript C:\Windows\System32\Scregedit.wsf /au 1
```


Administrateur : C:\Windows\system32\cmd.exe
C:\>cscript c:\windows\System32\Scregedit.wsf /au /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update AUOptions
Aucune valeur définie.
C:\>cscript c:\windows\System32\Scregedit.wsf /au 4
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
Le Registre a été mis à jour.
C:\>cscript c:\windows\System32\Scregedit.wsf /au /v
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update AUOptions
Affichez les paramètres de Registre.
4
C:\>cscript c:\windows\System32\Scregedit.wsf /au 1
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.
Le Registre a été mis à jour.
C:\>_

Vous pouvez forcer la vérification immédiate des mises à jour en exécutant `wuauclt /detectnow`.

Vous pouvez forcer l'installation immédiate des mises à jour en exécutant `wuauclt /install`.

Malgré ces commandes, le service de mises à jour stocke la date et l'heure de la dernière vérification. Aussi, après la demande initiale, un temps d'attente est imposé. Pour accélérer le processus, vous pouvez supprimer la clé de registre contenant la date et l'heure de la dernière et prochaine vérification :

```
Anet stop wuauserv
Breg delete
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\
Auto Update" /f
Cnet start wuauserv
Dwuauclt /detectnow
```

Un délai de quelques minutes reste toutefois imposé.

Pour consulter la liste des mises à jour installées, utilisez la commande `wmic qfe list ou wmic qfe.systeminfo`

3. Sauvegarder le serveur

L'installation Core étant souvent utilisée en environnement hostile, il est parfois utile de pouvoir faire au moins des sauvegardes locales du système. La gestion des sauvegardes se fait en installant la fonctionnalité WindowsServerBackup : `start /wait ocsetup WindowsServerBackup`.

Pour déclencher manuellement une sauvegarde, il faut utiliser la commande `wbadmin`. Dans notre exemple, nous allons effectuer une sauvegarde des lecteurs C:\ sur le partage \\autreserveur\partages\sauvegardes :

```
wbadmin start backup -
backuptarget :\\autreserveur\partages\sauvegardes -
include:c: -allcritical -vssfull -quiet
```

Les chemins UNC peuvent être directement utilisés comme destination de la sauvegarde. Un dossier nommé « WindowsImageBackup » sera créé. Ensuite un sous dossier portant le nom du serveur sera automatiquement créé. Toute sauvegarde précédente sera automatiquement écrasée. La restauration complète peut être faite en utilisant le DVD d'installation (option restauration).

© ENI Editions - All rigths reserved

4. Sécurisation du stockage avec BitLocker

La plupart du temps, les serveurs sont dans un datacenter, souvent surnommé « bunker » afin de mettre en avant la sécurité physique qui est mise en œuvre (caméras, contrôles d'accès…). Ce niveau de sécurité n'est pas toujours possible, surtout dans le cadre des sites distants, avec parfois seulement quelques utilisateurs. Bien que le nombre d'utilisateurs reste souvent assez faible, il apparaît indispensable de déployer sur place un serveur, afin de fournir certains services localement, notamment un contrôleur de domaine ou un service DHCP. Dans le premier cas, le serveur a par défaut une copie du domaine et donc des mots de passe de tous les utilisateurs. Comme vu dans le second chapitre de cet ouvrage, la mise en place d'un RODC permet de pallier ce problème. Mais comment faire s'il s'agit d'un serveur de fichiers ou de bases de données ?

La fonctionnalité BitLocker permet de chiffrer les partitions du serveur nativement depuis Windows. Cela constitue une amélioration très notable pour la sécurité physique du serveur. Le vol du serveur ou de son stockage ne constitue plus un point de sécurité critique. Pour mettre en place BitLocker, le serveur doit posséder une puce TPM (*Trusted Platform Management*) sur la carte mère. Il faut tout d'abord installer la fonctionnalité avec cette commande :

```
start /wait ocsetup BitLocker
```

À la fin de l'installation, un redémarrage est nécessaire.

```
cscript %systemroot%\System32\manage-bde.wsf -tpm -turnOn
```

Vous devez ensuite donner un mot de passe en exécutant :

```
cscript %systemroot%\System32\manage-bde.wsf -tpm -o password
```

Vous pouvez ensuite procéder au chiffrement de la partition avec la commande :

```
cscript %systemroot%\System32\manage-bde.wsf -on c: -rp
```

© ENI Editions - All rigths reserved

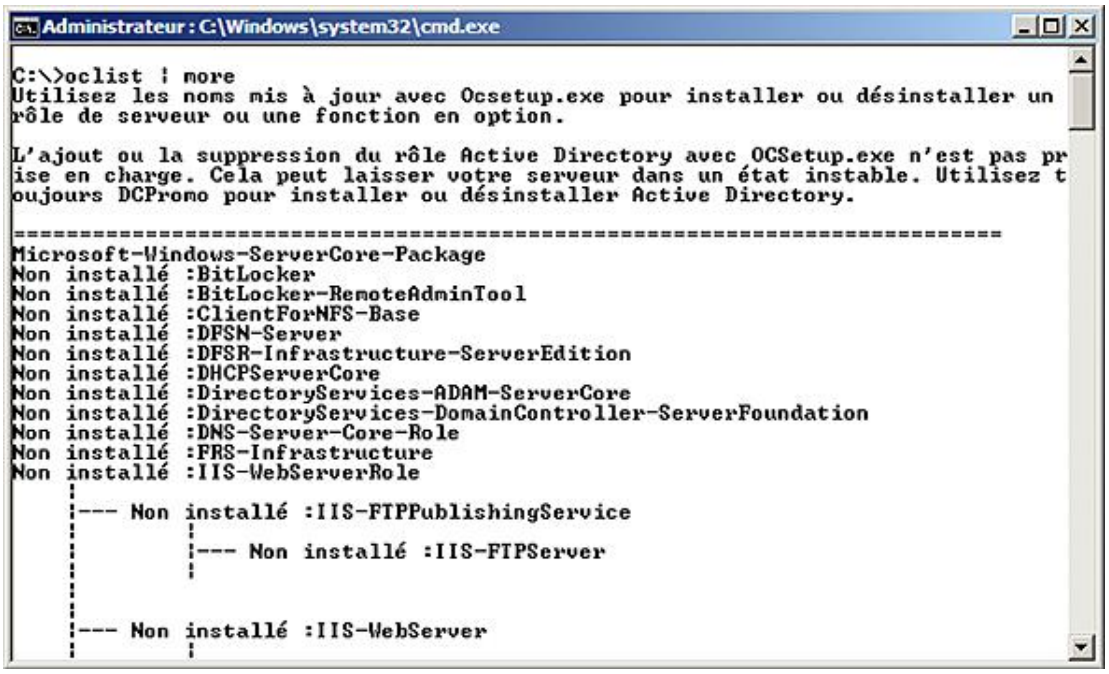
Mise en place d'un serveur Core et des applications associées

1. Installation des rôles et fonctionnalités

Contrairement à l'installation complète, l'utilitaire d'installation en ligne de commande `servermanagercmd` n'est pas disponible. À la place, il faut utiliser `oclist` et `ocsetup`. Le premier faisant un listing des rôles installés ou non, et le second permettant de les installer et de les supprimer.

Attention, ocsetup est sensible à la casse. Ainsi, ocsetup BitLocker échouera, alors que la commande ocsetup BitLocker fonctionnera.

Exemple de sortie écran avec `oclist` :


Administrateur : C:\Windows\system32\cmd.exe
C:\>oclist | more
Utilisez les noms mis à jour avec Ocsetup.exe pour installer ou désinstaller un rôle de serveur ou une fonction en option.
L'ajout ou la suppression du rôle Active Directory avec OCSetup.exe n'est pas pris en charge. Cela peut laisser votre serveur dans un état instable. Utilisez toujours DCPromo pour installer ou désinstaller Active Directory.
Microsoft-Windows-ServerCore-Package
Non installé :BitLocker
Non installé :BitLocker-RemoteAdminTool
Non installé :ClientForNFS-Base
Non installé :DFSN-Server
Non installé :DFSR-Infrastructure-ServerEdition
Non installé :DHCPServerCore
Non installé :DirectoryServices-ADAM-ServerCore
Non installé :DirectoryServices-DomainController-ServerFoundation
Non installé :DNS-Server-Core-Role
Non installé :FRS-Infrastructure
Non installé :IIS-WebServerRole
Non installé :IIS-FTPPublishingService
Non installé :IIS-FTPServer
Non installé :IIS-WebServer

a. Les rôles réseaux

L'installation des rôles réseaux se limite à une simple commande. Il est recommandé de les démarrer avec `start /w` afin de ne pas avoir un retour au prompt avant que l'installation ne soit effectivement terminée. Voici les commandes permettant l'installation des différents rôles réseaux disponibles. Ces rôles sont peu consommateur en ressources systèmes mais sont nécessaire en permanence. Utiliser une installation minimale permet de les sécuriser, et limiter les coupures de services grâce à la réduction du nombre de mises à jour de sécurités à installer.

Installer le rôle DHCP Server

```
start /w ocsetup DHCPServerCore
sc config dhcpserver start=auto
net start dhcpserver
```

Pour autoriser le serveur DHCP, exécutez :

```
netsh dhcp add server dc2008.masociete.local 192.168.4.15
```

Si le serveur devient contrôleur de domaine par la suite, il faudra l'autoriser de nouveau.

Pour créer un scope sur le serveur DHCP :

```
netsh dhcp server add scope 192.168.4.0 255.255.255.0
```

© ENI Editions - All rigths reserved

```
"Scope de Ma Societe"
```

Pour définir une plage d'adresses IP :

```
netsh dhcp server scope 192.168.4.0 add iprange
192.168.4.100 192.168.4.250
```

Pour définir une plage d'exclusions :

```
netsh dhcp server scope 192.168.4.0 add excluderange
192.168.4.1 192.168.4.99
```

Pour fournir l'adresse IP de la passerelle par défaut et les serveurs DNS dans les baux DHCP :

```
netsh dhcp server scope 192.168.1.0 set optionvalue 003
ipaddress 192.168.4.254
netsh dhcp server scope 192.168.4.0 set optionvalue 006
ipaddress 192.168.4.15 192.168.4.16
```

Pour fournir le suffixe DNS dans le bail DHCP :

```
netsh dhcp server scope 192.168.4.0 set optionvalue 015
String masociete.local
```

Pour activer le scope :

```
netsh dhcp server scope 192.168.4.0 set state 1
```

Windows Server 2008 R2 inclura une synchronisation entre les serveurs DHCP primaires et secondaires (DHCP Failover).

Installer le rôle DNS server

Tout comme le rôle précédent, l'installation se résume à une simple commande :

```
start /w ocsetup DNS-Server-Core-Role
```

Pour ajouter une zone DNS primaire sur le serveur :

```
dnscmd /zoneadd masociete.local /primary
```

L'ajout manuel d'entrées est très simple. Par exemple, pour déclarer un second serveur DNS pour la zone :

```
dnscmd /recordadd madociete.local @ NS
dc02.masociete.local
```

La zone n'accepte pas par défaut les mises à jour dynamiques. Pour les autoriser, il faut utiliser la commande :

```
dnscmd /config masociete.local /allowupdate 1
```

Vous pouvez voir toutes les entrées d'une zone en ligne de commande :

```
dnscmd /zoneprint masociete.local
```

Pour lister toutes les zones déclarées sur le serveur :

```
dnscmd /enumzones
```

Windows Server 2008 R2 inclura la sécurisation du DNS (DNSSEC), permettant de vérifier que la source est digne de confiance pour la résolution et le transfert de zones. Une infrastructure de type PKI permettra de protéger les entrées DNS.

Installer le rôle IIS server

Depuis IIS 7.0, presque toutes les fonctionnalités sont vues comme des modules, l'objectif étant d'installer le strict

© ENI Editions - All rigths reserved

nécessaire, tant pour la sécurité que pour les performances. L'implémentation du rôle IIS est un peu particulière dans l'installation Core due à l'absence de Framework .Net. En attendant la version R2, il est toutefois pertinent de l'installer pour servir du contenu statique ou PHP. L'installation du rôle se fait en exécutant la commande :

```
start /w ocsetup IIS-WebServerRole
```

Cependant, seulement quelques composants sont installés par défaut :

- IIS-WebServer ;
- IIS-ApplicationDevelopment ;
- IIS-CommonHttpFeatures ;
- IIS-HealthAndDiagnostics ;
- IIS-Performance ;
- IIS-Security ;
- IIS-WebServerManagementTools.

Contrairement à l'installation complète, les composants suivants ne sont pas disponibles :

- IIS-ASPNET ;
- IIS-NetFxExtensibility ;
- IIS-ManagementConsole ;
- IIS-ManagementService ;
- IIS-LegacySnapIn ;
- IIS-FTPManagement ;
- WAS-NetFxEnvironment ;
- WAS-ConfigurationAPI.

Par exemple, pour installer le module PHP sur un Server Core :

- Téléchargez le zip php sur un partage depuis une machine ayant un navigateur Internet : http://www.php.net/downloads.php
- Décompressez le contenu et déplacez-le dans %SystemDrive%\PHP.
- Renommez le fichier **php.ini-recommended** en **php.ini** dans ce répertoire.
- Installez les composants suivants :
  - IIS-WebServer ;
  - IIS-CommonHttpFeatures ;
  - IIS-StaticContent ;

© ENI Editions - All rigths reserved

- IIS-DefaultDocument ;
- IIS-DirectoryBrowsing ;
- IIS-HttpErrors ;
- IIS-HttpLogging ;
- IIS-LoggingLibraries ;
- IIS-RequestMonitor ;
- IIS-RequestFiltering ;
- IIS-HttpCompressionStatic ;
- IIS-CGI ;
- IIS-WebServerManagementTools ;
- WAS-WindowsActivationService ;
- WAS-ProcessModel.

- Activez php dans IIS en ajustant la lettre de lecteur en fonction de votre environnement :

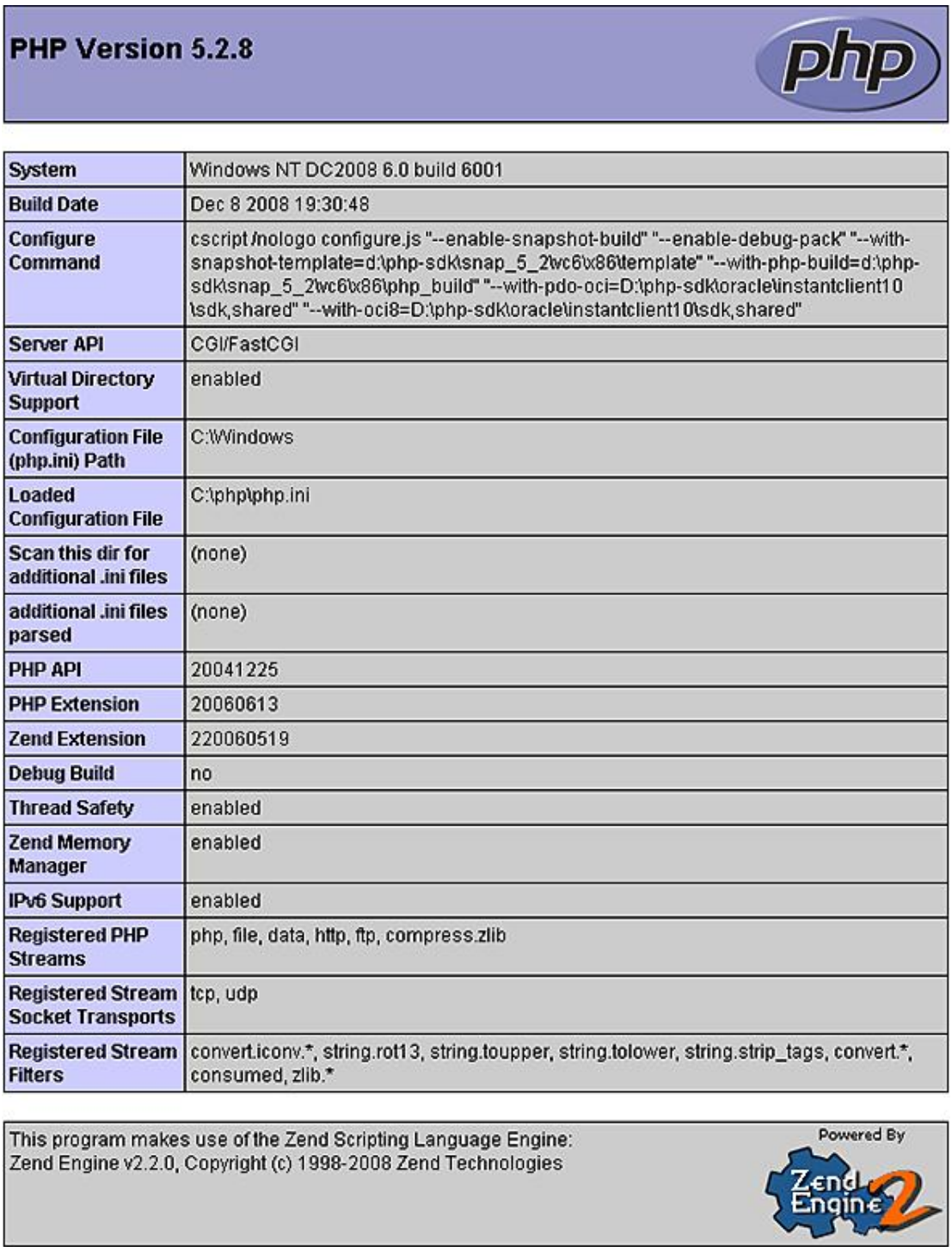
```
%WinDir%\System32\InetSrv\AppCmd set config
/section:system.webServer/fastCGI /+[fullPath='c:\php\php-
cgi.exe']

%WinDir%\System32\InetSrv\AppCmd set config
/section:system.webServer/handlers /+[name='PHP-
FastCGI',path='*.php',verb='*',modules='FastCgiModule',script
Processor='c:\php\php-cgi.exe',resourceType='Either']
```

Vous pouvez ensuite créer une page test.php avec à l'intérieur le code suivant, par exemple dans **%systemdrive%\inetpub\www\test.php** : `<?php phpinfo();?>`.

Une page semblable à celle-ci doit s'afficher :

© ENI Editions - All rigths reserved



PHP Version 5.2.8

System	Windows NT DC2008 6.0 build 6001
Build Date	Dec 8 2008 19:30:48
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared"
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\php\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2008 Zend Technologies

Powered By Zend Engine 2

b. Le rôle serveur de fichiers

Contrairement aux rôles réseaux, plusieurs services de rôles sont proposés, en fonction de vos besoins. Vous pouvez donc choisir d'installer ou non FRS, RFRS, DFS, SIS et même NFS. Le chapitre Architecture distribuée d'accès aux ressources de ce livre couvre en détail la gestion distribuée de ressources via DFS, ainsi nous allons ici nous intéresser aux spécificités liées à l'installation Core. Ce type d'installation est pertinent pour ce rôle, dont la disponibilité est vitale pour la plupart des utilisateurs. Davantage de mémoire peut être utilisée comme cache de fichiers grâce à l'empreinte plus faible, et la réduction du nombre de mises à jour réduit les coupures de services. La seule fonctionnalité manquante est la gestion des ressources (FSRM), mais Windows Server 2008 R2 comblera ce manque.

- Installation du service FRS :

```
start /w ocsetup FRS-Infrastructure
```

© ENI Editions - All rigths reserved

- Installation du service RFRS :

```
start /w ocsetup DFSR-Infrastructure-ServerEdition
```

- Installation du service DFS :

```
start /w ocsetup DFSN-Server
```

- Installation du service SIS (*Single Instance Storage*) :

```
start /w ocsetup SIS
```

Le service SIS permet de ne stocker qu'une seule instance d'un fichier de façon transparente pour les utilisateurs. Si trois utilisateurs enregistrent le même document Word dans trois dossiers par exemple.

- Installation du service NFS :

```
start /w ocsetup ServerForNFS-Base
```

```
start /w ocsetup ClientForNFS-Base
```

c. Le rôle serveur d'impressions

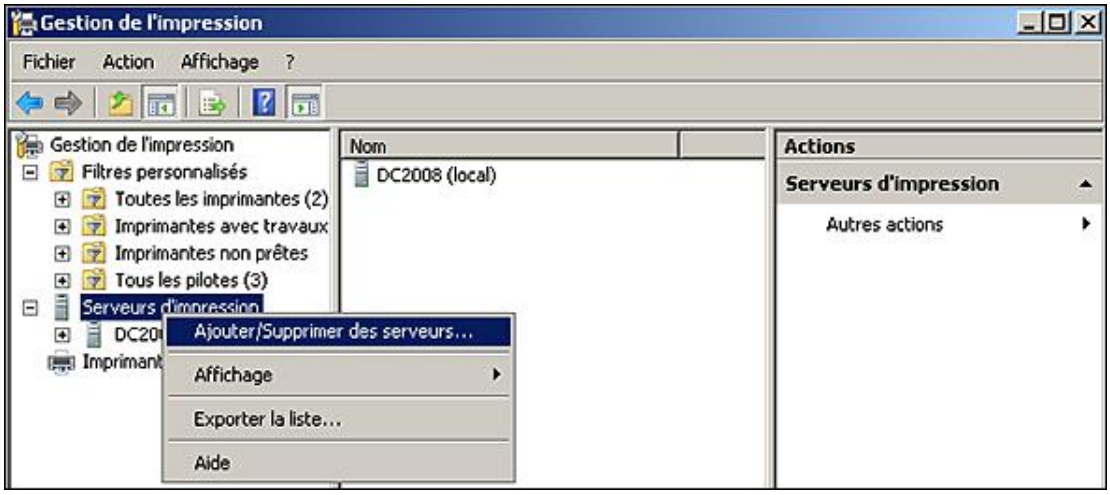
Le rôle de serveur d'impressions s'installe en une ligne de commande :

```
start /w ocsetup Printing-ServerCore-Role
```

Ajouter une imprimante sur le serveur :

Depuis un ordinateur Windows Vista ou un autre Windows Server 2008 non Core, lancez la console de **gestion des imprimantes**. Si elle n'est pas présente sur un Windows Server 2008, vous pouvez l'ajouter indépendamment avec la commande :

```
servermanagercmd -i RSAT-Print-Services
```



Il suffit ensuite de gérer le rôle comme sur l'édition complète.

2. Service d'annuaire (AD)

Contrairement aux autres rôles, il n'est pas possible de le configurer après son installation. Il faut lui fournir certaines informations au moment de l'installation, alors qu'il n'y a pas d'interface graphique. La solution consiste à passer par un fichier texte de réponses, qui doit être mis sur le serveur au préalable. Une fois le fichier de réponses prêt, il suffit d'exécuter la commande :

© ENI Editions - All rigths reserved

```
dcpromo /unattend:c:\monfichierunattend.txt
```

Voici quelques fichiers d'exemples afin de vous faciliter la création du fichier de réponses. Pour créer ces fichiers de réponses, vous pouvez utiliser notepad, qui est présent sur une installation Core (pratique, non ?).

Afin d'obtenir un contrôleur de domaine en lecture seule (RODC), il faut positionner `ReplicaOrNewDomain` à `ReadOnlyReplica`.

Fichier de réponses du premier serveur d'une nouvelle forêt :

```
[DCINSTALL]
ReplicaOrNewDomain=Domain
NewDomain=forest
InstallDNS=yes
NewDomainDNSName= masociete.local
DomainNetbiosName=masociete
ForestLevel=3
DomainLevel=3
SiteName=Default-First-Site-Name
DatabasePath=%systemroot%\ntds
LogPath=%systemroot%\ntds
SYSVOLPath=%systemroot%\sysvol
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=Yes
```

Fichier de réponses du premier serveur d'une nouvelle arborescence dans une forêt existante :

```
[DCINSTALL]
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
NewDomain=tree
NewDomainDNSName=masociete2.local
SiteName=Default-First-Site-Name
DomainNetBiosName= masociete2.local
ReplicaOrNewDomain=Domain
DomainLevel=3
DatabasePath="%systemroot%\NTDS"
LogPath="%systemroot%\NTDS"
SYSVOLPath="%systemroot%\SYSVOL"
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=administrateur
DNSDelegationPassword= Passw0rd
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

Fichier de réponses du premier serveur d'un nouveau domaine enfant dans une forêt existante :

```
[DCINSTALL]
ParentDomainDNSName=masociete.local
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
NewDomain=childChild
Name=masociete2
SiteName=Default-First-Site-Name
DomainNetBiosName=masociete2
ReplicaOrNewDomain=domain
DomainLevel=3
DatabasePath="%systemroot%\NTDS"
LogPath="%systemroot%\NTDS"
SYSVOLPath="%systemroot%\SYSVOL"
InstallDNS=yes
CreateDNSDelegation=yes
DNSDelegationUserName=administrateur
DNSDelegationPassword= Passw0rd
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

© ENI Editions - All rigths reserved

Fichier de réponses du second serveur d'un domaine :

```
[DCINSTALL]
UserName=administrateur
UserDomain=masociete
Password=Passw0rd
SiteName=Default-First-Site-Name
ReplicaOrNewDomain=replica
DatabasePath=”%systemroot%\NTDS”
LogPath=”%systemroot%\NTDS”
SYSVOLPath=”%systemroot%\SYSVOL”
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=Passw0rd
RebootOnCompletion=yes
```

Sachez également que ce fichier de configuration pourra être créé à l'issu de l'assistant d'installation d'un contrôleur de domaine en mode graphique.

© ENI Editions - All rigths reserved

Annexe : paramètres pour le fichier de réponse dcpromo

Voici la liste complète des paramètres possibles. Elle est également disponible ici : http://support.microsoft.com/kb/947034

1. Paramètres pour l'ajout d'un contrôleur de domaine

`AllowDomainReinstall`

- Yes | No
- Cette entrée indique si un domaine existant est recréé.

`AllowDomainControllerReinstall`

- Yes | No
- Cette entrée indique si l'installation de ce contrôleur de domaine doit se poursuivre même s'il existe un compte de contrôleur de domaine actif du même nom. Indiquez Yes uniquement si vous êtes sûr que le compte n'est plus utilisé.

`ApplicationPartitionsToReplicate`

- Aucune valeur par défaut.
- Cette entrée indique les partitions d'application qui doivent être répliquées au format ""partition1" "partition2"". Si * est indiqué, toutes les partitions d'application vont être répliquées. Utilisez des noms uniques séparés par des espaces ou séparés par des virgules et des espaces. Mettez la chaîne entière entre guillemets.

`ChildName`

- Aucune valeur par défaut.
- Il s'agit du nom du domaine subordonné qui est annexé à l'entrée ParentDomainDNSName. Si le domaine parent est A.COM et le domaine subordonné B, entrez B.A.COM et B pour ChildName.

`ConfirmGc`

- Yes | No
- Cette entrée indique si le réplica est également un catalogue global. Yes fait du réplica un catalogue global si la sauvegarde était un catalogue global. No ne fait pas du réplica un catalogue global.

`CreateDNSDelegation`

- Yes | No
- Aucune valeur par défaut.
- Cette entrée indique si une délégation DNS faisant référence à ce nouveau serveur DNS doit être créée. Valide uniquement pour le DNS intégré à AD DS.

`CriticalReplicationOnly`

- Yes | No

© ENI Editions - All rigths reserved

- Cette entrée indique si l'opération d'installation effectue seulement une réplication importante avant un redémarrage puis omet la partie réplication non critique et potentiellement longue. La réplication non critique après l'installation de rôle se termine, puis l'ordinateur redémarre.

`DatabasePath`

- %systemroot%\NTDS

- Il s'agit du chemin du répertoire non UNC (convention d'affectation des noms) complet sur un disque dur de l'ordinateur local. Ce répertoire doit héberger la base de données AD DS (NTDS.DIT). Si ce répertoire existe, il doit être vide. Dans le cas contraire, il sera créé. L'espace disque sur le lecteur logique sélectionné doit être de 200 mégaoctets (MB). Pour appliquer les erreurs d'arrondi ou tous les objets du domaine, davantage d'espace disque libre peut être nécessaire. Pour de meilleures performances, choisissez un répertoire situé sur un disque dur dédié.

`DelegatedAdmin`

- Aucune valeur par défaut

- Cette entrée indique le nom de l'utilisateur ou du groupe qui va installer et administrer le contrôleur de domaine en lecture seule. Si aucune valeur n'est indiquée, seuls les membres du groupe Administrateurs de domaine ou Administrateurs d'entreprise peuvent installer et administrer le contrôleur de domaine en lecture seule.

`DNSDelegationPassword`

- <Password> | *

- Aucune valeur par défaut.

- Cette entrée indique le mot de passe du compte d'utilisateur utilisé pour créer ou supprimer la delegation DNS. Indiquez * pour inviter l'utilisateur à entrer des informations d'identification.

`DNSDelegationUserName`

- Aucune valeur par défaut.

- Cette entrée indique le nom d'utilisateur à utiliser lors de la création ou de la suppression de la délégation DNS. Si vous n'indiquez pas de valeur, les informations d'identification de compte que vous indiquez pour l'installation ou la suppression de AD DS sont utilisées pour la délégation DNS.

`DNSOnNetwork`

- Yes | No

- Cette entrée indique si le service DNS est disponible sur le réseau. Elle est utilisée uniquement lorsque l'adaptateur réseau de cet ordinateur n'est pas configuré pour utiliser le nom d'un serveur DNS pour la résolution de nom. Indiquez No pour préciser que DNS doit être installé sur cet ordinateur pour la résolution de nom. Dans le cas contraire, l'adaptateur réseau doit être configuré pour utiliser d'abord le nom de serveur DNS.

`DomainLevel`

- 0 | 2 | 3

- Aucune valeur par défaut.

- Cette entrée indique le niveau fonctionnel du domaine. Cette entrée est basée sur les niveaux qui existent dans la forêt lorsqu'un nouveau domaine est créé dans une forêt existante. Les descriptions des valeurs sont les suivantes :

© ENI Editions - All rigths reserved

- 0 = Mode Windows 2000 Server natif
- 2 = Windows Server 2003
- 3 = Windows Server 2008

`DomainNetbiosName`

- Aucune valeur par défaut.
- Cette entrée est le nom NetBIOS qui est utilisé par des clients antérieurs à AD DS pour l'accès au domaine. DomainNetbiosName doit être unique sur le réseau.

`ForestLevel`

- 0 | 2 | 3
- Cette entrée indique le niveau fonctionnel de la forêt lorsqu'un nouveau domaine est créé dans une nouvelle forêt comme suit :
  - 0 = Windows 2000 Server
  - 2 = Windows Server 2003
  - 3 = Windows Server 2008

  Vous ne devez pas utiliser cette option lors de l'installation d'un nouveau contrôleur de domaine dans une forêt existante. L'option **ForestLevel** remplace l'option **SetForestVersion** qui est disponible dans Windows Server 2003.

`InstallDNS`

- Yes | No
- La valeur par défaut change en fonction de l'opération. Pour une nouvelle forêt, le rôle de serveur DNS est installé par défaut. Pour une nouvelle arborescence, un nouveau domaine enfant ou un réplica, un serveur DNS est installé par défaut si une infrastructure DNS existante est détectée par l'Assistant Installation des services de domaine Active Directory. Si aucune infrastructure DNS existante n'est détectée par l'assistant, aucun serveur DNS n'est installé par défaut.
- Cette entrée indique si le DNS est configuré pour un nouveau domaine lorsque l'Assistant Installation des services de domaine Active Directory détecte que le protocole de mise à jour dynamique DNS n'est pas disponible. Cette entrée s'applique également si l'assistant détecte un nombre insuffisant de serveurs DNS pour un domaine existant.

`LogPath`

- %systemroot%\NTDS
- Il s'agit du chemin du répertoire non UNC (convention d'affectation des noms) complet sur un disque dur de l'ordinateur local qui va héberger les fichiers journaux AD DS. Si ce répertoire existe, il doit être vide. Dans le cas contraire, il sera créé.

`NewDomain`

- Tree | Child | Forest
- Tree signifie que le nouveau domaine est la racine d'une nouvelle arborescence dans une forêt existante. Child signifie que le nouveau domaine est un enfant d'un domaine existant. Forest signifie que le nouveau domaine est le premier domaine dans une nouvelle forêt d'arborescences de domaines.

© ENI Editions - All rigths reserved

`NewDomainDNSName`

- Aucune valeur par défaut.
- Cette entrée est utilisée dans les installations « nouvelle arborescence dans une forêt existante » ou « nouvelle forêt ». La valeur est un nom de domaine DNS qui n'est pas actuellement utilisé.

`ParentDomainDNSName`

- Aucune valeur par défaut.
- Cette entrée indique le nom d'un domaine DNS parent existant pour une installation de domaine enfant.

`Mot de passe`

- <Password> | *
- Aucune valeur par défaut.
- Cette entrée indique le mot de passe qui correspond au compte d'utilisateur utilisé pour configurer le contrôleur de domaine. Indiquez * pour inviter l'utilisateur à entrer des informations d'identification. Pour garantir une protection, les mots de passe sont retirés du fichier de réponses après une installation. Les mots de passe doivent être redéfinis chaque fois qu'un fichier de réponses est utilisé.

`PasswordReplicationAllowed`

- <Security_Principal> | NONE
- Aucune valeur par défaut.
- Cette entrée indique les noms des comptes d'ordinateur et des comptes d'utilisateur dont les mots de passe peuvent être répliqués sur ce contrôleur de domaine en lecture seule. Indiquez NONE si vous voulez n'indiquer aucune valeur. Par défaut, aucune information d'identification ne sera mise en cache sur ce contrôleur de domaine en lecture seule. Pour indiquer plusieurs entités de sécurité, ajoutez l'entrée plusieurs fois.

`PasswordReplicationDenied`

- <Security_Principal> | NONE
- Cette entrée indique les noms des comptes d'utilisateur, des comptes de groupe et des comptes d'ordinateur dont les mots de passe ne doivent pas être répliqués sur le contrôleur de domaine en lecture seule. Indiquez NONE si vous ne voulez pas refuser la réplication des informations d'identification pour des utilisateurs ou des ordinateurs. Pour indiquer plusieurs entités de sécurité, ajoutez l'entrée plusieurs fois.

`RebootOnCompletion`

- Yes | No
- Cette entrée indique si l'ordinateur doit être redémarré après l'installation ou la suppression de AD DS que l'opération aboutisse ou non.

`RebootOnSuccess`

- Yes | No | NoAndNoPromptEither
- Cette entrée indique si l'ordinateur doit être redémarré après que l'opération d'installation ou de suppression de AD DS a abouti. Un redémarrage est toujours requis pour terminer une modification dans un rôle AD DS.

© ENI Editions - All rigths reserved

`ReplicaDomainDNSName`

- Aucune valeur par défaut.
- Cette entrée indique que le nom complet du domaine (FQDN) dans lequel vous voulez configurer un contrôleur de domaine supplémentaire.

`ReplicaOrNewDomain`

- Replica | ReadOnlyReplica | Domain
- Cette entrée est utilisée uniquement pour les nouvelles installations. Domain indique que le serveur est converti en premier contrôleur de domaine d'un nouveau domaine. ReadOnlyReplica permet de convertir le serveur en contrôleur de domaine en lecture seule. Replica permet de convertir le serveur en contrôleur de domaine supplémentaire.

`ReplicationSourceDC`

- Aucune valeur par défaut.
- Cette entrée indique le nom de domaine complet du contrôleur de domaine partenaire à partir duquel les données AD DS sont répliquées pour créer le nouveau contrôleur de domaine.

`ReplicationSourcePath`

- Aucune valeur par défaut.
- Cette entrée indique l'emplacement des fichiers d'installation qui sont utilisés pour créer un nouveau contrôleur de domaine.

`SafeModeAdminPassword`

- <Password> | NONE
- Aucune valeur par défaut.
- Cette entrée est utilisée pour fournir le mot de passe du compte d'administrateur hors connexion qui est utilisé en mode restauration Active Directory. Vous ne pouvez pas indiquer un mot de passe à blanc.

`SiteName`

- Premier-Site-par-défaut
- Cette entrée indique le nom de site lors de l'installation d'une nouvelle forêt. Pour une nouvelle forêt, la valeur par défaut est Premier-Site-par-défaut. Pour tous les autres scénarios, un site est sélectionné à partir du site en cours et de la configuration de sous-réseau de la forêt.

`SkipAutoConfigDNS`

- Aucune valeur par défaut.
- Cette option est destinée aux utilisateurs experts qui souhaitent omettre la configuration automatique des paramètres du client, des redirecteurs et des indications de racine. Cette option est appliquée uniquement si le service Serveur DNS est déjà installé sur le serveur. Dans ce cas, vous devez recevoir un message d'information qui confirme que la configuration automatique du DNS a été omise. Dans le cas contraire, cette option est ignorée. Si vous indiquez ce commutateur, assurez-vous que des zones sont créées et configurées correctement avec l'installation de AD DS, ou bien le contrôleur de domaine ne fonctionnera pas correctement. Cette option n'omet pas la création automatique de la délégation DNS dans la zone DNS parente. Pour contrôler la création de délégation DNS, utilisez l'option **DNSDelegation**.

© ENI Editions - All rigths reserved

`Syskey`

- <system_key> | NONE
- Cette entrée indique la clé système du support à partir duquel vous répliquez les données.

`SYSVOLPath`

- %systemroot%\SYSVOL
- Cette entrée indique un répertoire non UNC complet sur le disque dur de l'ordinateur local. Ce répertoire doit héberger les fichiers journaux de AD DS. Si ce répertoire existe déjà, il doit être vide. Dans le cas contraire, il sera créé. Le répertoire doit se trouver sur une partition qui a été formatée à l'aide du système de fichiers NTFS 5.0. Pour de meilleures performances, placez ce répertoire sur un autre disque dur que le système d'exploitation.

`TransferIMRoleIfNeeded`

- Yes | No
- Cette entrée indique si le rôle de maître de l'infrastructure doit être transféré sur ce contrôleur de domaine. Cette option est utile si le contrôleur de domaine est actuellement hébergé sur un serveur de catalogue global, et si vous n'envisagez pas de faire du contrôleur de domaine un serveur de catalogue global. Indiquez Yes pour transférer le rôle de maître de l'infrastructure sur ce contrôleur de domaine. Si vous indiquez Yes, pensez à préciser l'option ConfirmGC=No.

`UserDomain`

- Aucune valeur par défaut.
- Cette entrée indique le nom de domaine pour le compte d'utilisateur utilisé pour installer AD DS sur un serveur.

`UserName`

- Aucune valeur par défaut.
- Cette entrée indique le nom de compte d'utilisateur utilisé pour installer AD DS sur un serveur. Nous vous recommandons d'indiquer les informations d'identification de compte au format <domaine>\<nom_utilisateur>.

2. Paramètres pour la suppression d'un contrôleur de domaine

`AdministratorPassword`

- Aucune valeur par défaut.
- Cette entrée est utilisée pour indiquer le mot de passe administrateur local lors de la suppression de AD DS à partir d'un contrôleur de domaine.

`DemoteFSMO`

- Yes | No
- Indique qu'une suppression forcée a lieu même si un rôle de maître des opérations est tenu par le contrôleur de domaine.

`DNSDelegationPassword`

© ENI Editions - All rigths reserved

- <Password> | *
- Aucune valeur par défaut.
- Cette entrée indique que le mot de passe du compte d'utilisateur utilisé pour créer ou pour supprimer la délégation DNS. Indiquez * pour inviter l'utilisateur à entrer des informations d'identification.

`DNSDelegationUserName`

- Aucune valeur par défaut.
- Cette entrée indique le nom d'utilisateur à utiliser lors de la création ou de la suppression de la délégation DNS. Si vous n'indiquez pas de valeur, les informations d'identification de compte que vous indiquez pour l'installation ou la suppression de AD DS sont utilisées pour la délégation DNS.

`IgnoreIsLastDcInDomainMismatch`

- Yes | No
- Cette entrée indique que la suppression de AD DS doit se poursuivre à partir du contrôleur de domaine lorsque l'option IsLastDCInDomain=Yes est spécifiée ou lorsque l'Assistant Installation des services de domaine Active Directory détecte qu'il existe un autre contrôleur de domaine actif dans le domaine. Cette entrée s'applique également à un scénario dans lequel l'option IsLastDCInDomain=No est spécifiée, et/ou l'assistant ne peut pas contacter un autre contrôleur de domaine dans le domaine.

`IgnoreIsLastDNSServerForZone`

- Yes | No
- Cette entrée indique si la suppression de AD DS doit se poursuivre même si le contrôleur de domaine est le dernier serveur DNS pour une ou plusieurs zones intégrées à AD DS hébergées par le contrôleur de domaine.

`IsLastDCInDomain`

- Yes | No
- Cette entrée indique que le contrôleur de domaine à partir duquel vous supprimez AD DS est le dernier contrôleur de domaine dans le domaine.

`Mot de passe`

- <Password> | *
- Aucune valeur par défaut.
- Cette entrée indique le mot de passe qui correspond au compte d'utilisateur utilisé pour configurer le contrôleur de domaine. Indiquez * pour inviter l'utilisateur à entrer des informations d'identification. Pour garantir une protection, les mots de passe sont retirés du fichier de réponses après l'installation de AD DS. Les mots de passe doivent être redéfinis chaque fois qu'un fichier de réponses est utilisé.

`RebootOnCompletion`

- Yes | No
- Cette entrée indique si l'ordinateur doit être redémarré après l'installation ou la suppression de AD DS que l'opération aboutisse ou non.

`RebootOnSuccess`

- Yes | No | NoAndNoPromptEither

© ENI Editions - All rigths reserved

- Détermine si l'ordinateur doit être redémarré après que l'opération d'installation ou de suppression de AD DS a abouti. Un redémarrage est toujours requis pour terminer une modification dans un rôle AD DS.

`RemoveApplicationPartitions`

  - Yes | No
  - Cette entrée indique si les partitions d'application doivent être supprimées lors de la suppression de AD DS à partir d'un contrôleur de domaine. Yes indique que des partitions d'application sont retirées sur le contrôleur de domaine. No indique que des partitions d'application ne sont pas retirées sur le contrôleur de domaine. Si le contrôleur de domaine héberge le dernier réplica d'une partition de l'annuaire d'application, vous devez confirmer manuellement que vous devez supprimer ces partitions.

`RemoveDNSDelegation`

  - Yes | No
  - Cette entrée indique si les délégations DNS qui pointent sur ce serveur DNS doivent être supprimées à partir de la zone DNS parente.

`RetainDCMetadata`

  - Yes | No
  - Cette entrée indique si les métadonnées du contrôleur de domaine sont conservées dans le domaine après la suppression de AD DS, de sorte qu'un administrateur délégué puisse supprimer AD DS à partir d'un contrôleur de domaine en lecture seule.

`UserDomain`

- Aucune valeur par défaut.
- Cette entrée indique le nom de domaine pour le compte d'utilisateur utilisé pour installer AD DS.

`UserName`

  - Aucune valeur par défaut.
  - Cette entrée indique le nom de compte d'utilisateur utilisé pour installer AD DS sur un serveur. Nous vous recommandons d'indiquer les informations d'identification de compte au format <domaine>\<nom_utilisateur>.

Vous avez maintenant un serveur Core complètement fonctionnel dans votre environnement. Certains usages ont été présentés, d'autres comme Hyper-V sont décrit dans le chapitre Consolider vos serveurs avec Hyper V de cet ouvrage. Les avantages de cette installation minimum sont réels, la difficulté principale étant d'appréhender son administration au quotidien. Windows Server 2008 R2 permettra de lever certaines restrictions, notamment liées à l'absence du Framework .Net, permettant ainsi encore plus d'usages. Server Core, la fin du clivage interface Windows versus shell Unix ?

© ENI Editions - All rigths reserved

Introduction

Ce chapitre est dédié à la solution de virtualisation Microsoft, Hyper-V. Contrairement aux produits précédents de Microsoft sur le sujet, comme Virtual Server, la virtualisation a été pensée dès la conception du système d'exploitation. Ce véritable hyperviseur est même disponible gratuitement (sans achat de licence Windows Server 2008) chez Microsoft. Dans ce chapitre, vous découvrirez comment rentabiliser davantage votre infrastructure existante et la rendre plus souple aux changements.

© ENI Editions - All rigths reserved

Pourquoi consolider ?

La virtualisation est de plus en plus répandue dans les entreprises. Elle ne doit pas pour autant être systématique. Avant de lancer un projet de virtualisation, vous devez en mesurer toutes les conséquences ainsi que tous les avantages potentiels. Comme pour beaucoup de choses, il est recommandé de penser grand mais commencer petit.

1. Virtuel versus Physique

En première approche, virtualiser permet de s'affranchir des contraintes matérielles, tout en permettant un meilleur rendement. L'approche par des serveurs physiques est la plus simple au départ, mais elle se complique avec la quantité. En plus de la maintenance des systèmes d'exploitation et applications, il faut gérer le cycle de vie du matériel :

- Pannes matérielles
- Mises à jour des bios, firmwares, pilotes
- Cycles d'amortissements

Bien sûr, les solutions à ces problèmes sont bien connues et peuvent tout à fait être gérées dans les règles de l'art. Mais il y a toujours ce nouveau modèle de serveurs qui vient en remplacement du précédent, pour lequel votre image d'installation de Windows ne contient pas le bon pilote. La virtualisation vous propose de masquer cette gestion afin de vous consacrer à des tâches ayant plus de valeur ajoutée.

a. Optimisation des coûts

Un des objectifs de la virtualisation est la réduction des coûts d'infrastructures. Pour y parvenir, un des grands axes est l'optimisation des ressources disponibles. Les capacités des serveurs continuent d'évoluer de façon importante, mais les besoins applicatifs ne suivent pas toujours la même progression. Même le serveur le moins cher proposé chez les constructeurs a au moins un processeur double ou quadruple cœurs, quelques Giga de mémoire vive et du stockage SAS conséquent. Si un serveur héberge une ou même plusieurs applications, il n'utilisera sûrement qu'un modeste pourcentage de ces ressources. La plupart des éditeurs continuent par ailleurs à demander un serveur « dédié » pour assurer le support de leurs logiciels. Il en résulte des salles machines contenant beaucoup de serveurs, mais chacun d'eux utilisé à moins de 10 % de leur capacité. La virtualisation permet de maintenir un cloisonnement logique, dans un système d'exploitation dédié, tout en mutualisant l'infrastructure matérielle. Cette mutualisation physique a déjà un impact fort sur les coûts :

- Réduction de l'ensemble des coûts liés à la salle machine : électrique, climatique, câblages, encombrement au sol…
- Réduction des coûts de maintenance, proportionnellement aux nombres de serveurs physiques économisés.

La virtualisation réduit aussi les coûts liés à l'ajout d'un nœud dans l'infrastructure. La génération d'une machine virtuelle n'entraîne pas de coûts de câblage informatique, mise en rack… Cette économie prend tout son sens dans un environnement où le nombre de demandes est important, comme dans les environnements de développement et de recette. La solution SCVMM (*System Center Virtual Machine Manager*) permet même l'implémentation d'un portail libre service pour la création de machines virtuelles à la demande.

Un usage un peu moins conventionnel est d'utiliser la virtualisation pour maintenir en fonctionnement des systèmes vieillissant, dont le matériel qui les héberge n'est plus maintenu ou maintenable. La plupart des systèmes d'informations possèdent quelques systèmes obsolètes, avec des applications pour lesquelles ils n'ont pas de documentation ni les sources. Les migrer en machines virtuelles permet de les maintenir dans le système d'information tout en évitant les problèmes matériels.

b. Les limites de la virtualisation

Tout n'est pas forcément un bon candidat à la virtualisation. La solution Hyper-V ne supporte pas l'ensemble des systèmes d'exploitation Microsoft par exemple. L'article 954958 de la base de connaissance recense les versions serveurs et clientes supportées par Hyper-V. Au moment de l'écriture de cet ouvrage, les versions suivantes sont supportées :

Côté serveur :

© ENI Editions - All rigths reserved

- Windows 2003 SP2, 2008 en 32 et 64 bits ;
- Windows 2000 Server Service pack 4 ;
- SUSE Linux Enterprise Server 10 Service pack 1 et 2, en 32 et 64 bits.

Côté client :

- Windows XP SP2 et SP3, Vista SP1 en 32 et 64 bits.

Certains éditeurs ne supportent pas encore leur progiciel en environnement virtuel. Microsoft tient pour sa part la liste de leurs logiciels supportés en environnement virtuel avec Hyper-V : http://support.microsoft.com/kb/957006

Ainsi que ceux qui ne le sont pas (à ce jour, les autres solutions de virtualisation Microsoft dans des VM ainsi que le rôle serveur de fax Microsoft) : http://support.microsoft.com/kb/958664

Certains éléments d'architecture ne doivent pas cohabiter sur la même infrastructure, notamment à des fins de disponibilité. Par exemple, deux serveurs DNS ou DHCP ne devraient pas être sur le même serveur Hyper-V. Dans le cas contraire, en cas de défaillance de celui-ci, ces services deviennent indisponibles en même temps, alors qu'ils sont présents deux fois sur le réseau afin d'être très disponibles. Des services différents qui ont une forte activité en même temps devraient être sur des serveurs Hyper-V différents, afin de ne pas charger négativement l'infrastructure virtuelle. Des règles d'affinités et d'anti affinités devraient être définies. Enfin, les solutions nécessitant des cartes matérielles (cartes numéris, accès primaire…) ou les solutions utilisant des dongles sont très difficiles à migrer en environnement virtuel. Les ports COM du serveur physique ne sont pas accessibles depuis les machines virtuelles, tout comme le lecteur de disquettes.

2. De nouvelles problématiques

Il serait illusoire de penser que la virtualisation n'amène que des avantages et aucun inconvénient. Comme toute solution technique, l'important est de la maîtriser, quelle qu'elle soit, afin d'en tirer parti. Deux sujets au moins nécessitent une attention particulière : les impacts de la mutualisation et la sauvegarde.

a. Environnement mutualisé

La mutualisation est un axe classique de rentabilisation, mais il devient beaucoup plus sensible avec la virtualisation, car poussé à l'extrême. Elle part du postulat que la plupart des systèmes ne consomment pas les ressources matérielles qui leurs sont disponibles et les mutualisent donc à plusieurs pour rentabiliser ces ressources. Sauf que nous pouvons rarement prévoir la charge que vont générer les utilisateurs sur l'ensemble des systèmes virtuels à un instant T. Il se peut donc que plusieurs VM veuillent soudainement consommer le maximum disponible, perturbant ainsi les autres VM. La performance peut rapidement devenir un frein à la virtualisation si elle n'est pas gérée correctement. Le phénomène classique étant que les utilisateurs constatent des lenteurs, qu'ils associent immédiatement au fait qu'il s'agit d'une machine virtuelle. Ils deviennent ainsi réfractaires à leur utilisation, pensant que c'est la cause unique de ces lenteurs. D'autant que ce type de problème peut apparaître de façon insidieuse avec le temps. Elle apparaît aussi quand, au contraire, les performances sont là et que le succès de la solution incite à mettre en service plus de machines virtuelles que le dimensionnement de l'infrastructure ne le prévoyait. Tout projet de virtualisation devrait avoir un plan de capacité, maintenu à jour en permanence. Si le système à virtualiser est déjà en cours d'utilisation, historiez au maximum l'utilisation des ressources au préalable. Cela permettra de prédire son impact sur l'infrastructure Hyper-V ainsi que les ressources à y allouer. Hyper-V permet de limiter la consommation de chaque machine virtuelle, ainsi que de garantir une certaine quantité de ressource à tout instant. La réservation de ressource a l'inconvénient de bloquer la ressource, même si la machine virtuelle ne l'utilise pas. La limite permet de restreindre une machine virtuelle qui est soit non critique, comme une machine de test, soit qui consomme toutes les ressources disponibles, comme un serveur de traitements massifs. Vous pouvez aussi attribuer un poids à chaque machine virtuelle, permettant ainsi de prioriser l'accès aux ressources disponibles qui ne sont pas réservées. Si deux machines virtuelles demandent plus de ressource processeur en même temps par exemple, celle qui a le plus de poids sera prioritaire. Vous pouvez allouer de 1 à 4 processeurs virtuels à chaque machine virtuelle, du moment que vous avez le nombre de cœurs physiques correspondants. Sur un serveur physique ayant quatre cœurs, chaque VM peut donc avoir quatre processeurs logiques. Les serveurs actuels ont généralement au moins deux voir quatre cœurs, ce qui est le plus rentable pour la virtualisation. Si vous assignez à chaque VM deux processeurs logiques, cela permet de maintenir un temps de réponse correct sur la VM, même si un processeur logique est consommé en entier par un programme ou un traitement. Si vous n'allouez qu'un seul processeur logique et qu'un thread consomme tous les cycles en boucle, il vous sera peut être même difficile d'accéder au système pour stopper ce processus. Ce phénomène est aussi vrai sur une machine physique avec un seul cœur, mais il est amplifié par la virtualisation, et n'est plus présent dans l'esprit des utilisateurs qui ont généralement au moins deux cœurs sur leur station (hyper threading ou dual core).

La perte d'un serveur physique Hyper-V a des conséquences beaucoup plus graves qu'un serveur sans virtualisation. En effet, ce type de serveur héberge potentiellement plusieurs VM (dizaine ?), qui vont toutes être

© ENI Editions - All rigths reserved

indisponibles en même temps. Il faut donc être préparé à ce scénario, afin de prendre de bonnes décisions, comme l'ordre dans lequel remettre en service ces VM. Il est recommandé de déployer au moins deux serveurs Hyper-V, afin d'avoir un plan de reprise rapide en cas de défaillance grave d'un des deux serveurs.

b. Sauvegarde

La sauvegarde d'une infrastructure virtuelle est un sujet d'attention particulier. Plusieurs implémentations sont possibles, vous devrez trouver celle qui vous apporte le plus de souplesse, tout en limitant les contraintes et coûts associés. Votre objectif doit être de répondre à vos besoins, de la manière la plus adaptée dans votre contexte, en respectant vos engagements de services auprès de vos clients.

Trois grands axes de sauvegarde sont possibles :

- Traiter les machines virtuelles comme s'ils s'agissaient de serveurs standards, en installant l'agent de sauvegarde traditionnel sur chaque machine virtuelle.
- Implémenter une sauvegarde en utilisant les possibilités offertes par l'infrastructure virtuelle.
- Sauvegarder les disques virtuels des machines virtuelles à froid, c'est-à-dire VM arrêtées.

La première solution a l'avantage d'être très classique, mais elle est aussi sûrement la plus coûteuse, car elle n'apporte pas d'économie liée à la virtualisation. Certains éditeurs de solution de sauvegarde proposent cependant un prix par agent inférieur quand il s'agit de machines virtuelles.

Nous allons nous attacher aux solutions de sauvegardes qui prennent en compte les fonctionnalités offertes par la virtualisation. Une machine virtuelle peut avoir plusieurs états :

- Allumée ou Éteinte ;
- En pause ;
- Avec une ou plusieurs images instantanées (ou aucune).

Les images instantanées permettent de prendre une « photo » de la VM à un instant T. Pour cela, Hyper-V va créer un nouveau disque virtuel (*.avhd) qui contiendra toutes les différences générées après cette image. Cela ne constitue pas pour autant un mécanisme de sauvegarde à lui tout seul. Le fichier maître est indispensable pour son fonctionnement, et ne peut donc pas être sorti de la VM. Cette fonctionnalité n'est pas disponible pour les disques physiques attachés directement à la VM (pass-through). Pour certains rôles, comme le contrôleur de domaine, cette fonctionnalité n'est même pas supportée par Microsoft. En revanche, cette fonctionnalité est vraiment un « must » par ailleurs. Le nombre maximum d'image instantanée est de 50 par machine virtuelle.

Les sauvegardes à froid sont les plus simples, mais impliquent un temps d'arrêt, qui n'est pas toujours possible. Un redémarrage du système d'exploitation peut générer des pertes de performances si un cache en mémoire est utilisé (SQL Server…).

Votre solution de sauvegarde peut proposer un agent de sauvegarde pour Hyper-V. Ce mécanisme utilise la technologie VSS (*Volume Shadowcopy Service*). Vous obtiendrez ainsi des copies des machines virtuelles autonomes, que vous pouvez déplacer ou conserver sur bande, sans temps d'arrêt. La solution de sauvegarde Microsoft DPM (*Data Protection Manager*) ainsi que la solution de sauvegarde native Windows Server 2008 sont compatibles avec ce type de sauvegarde. Pour que ce type de solution fonctionne, certains pré-requis doivent être remplis :

- Les outils « services d'invité virtuel » doivent être installés et le service « backup integration » doit être actif.
- Tous les volumes utilisés par la VM doivent être en mode basique et formatés en NTFS.
- Le service Windows VSS doit être actif sur tous les volumes et chaque volume doit avoir son stockage VSS sur lui-même.

Si une sauvegarde en ligne ne peut pas être effectuée, alors une sauvegarde à froid de la machine sera effectuée. Pour cela, son état sera sauvegardé, et une fois la sauvegarde terminée, elle sera mise de nouveau dans l'état antérieur à la sauvegarde. Ce type de sauvegarde permet de restaurer entièrement une machine virtuelle, mais pas une sous partie de celle-ci (comme un fichier du disque C:\ dans cette machine). Il ne faut pas lancer de sauvegarde ou de restauration à la fois sur une machine virtuelle et sur la partition racine. Vous pourriez générer des conflits si chaque instance essaye de verrouiller l'enregistreur VSS.

© ENI Editions - All rigths reserved

Voici une commande pour sauvegarder tout un serveur Hyper-V ainsi que l'ensemble des machines virtuelles à chaud :

```
wbadmin start backup -backuptarget:\\
autreserveur\partages\sauvegardes -include:c:,d: -
allcritical -vssfull -quiet
```

3. Préparer son déploiement

a. Pré-requis

Pour pouvoir porter le rôle Hyper-V, un serveur physique doit avoir un processeur 64 bits avec des fonctionnalités de virtualisation (Intel-VT ou AMD-V) et de sécurité (Intel XD ou AMD NX). Hyper-V supporte jusqu'à 16 processeurs sur le serveur physique, qu'ils proviennent de cœurs physiques ou logiques via hyper threading.

Une installation minimale (Core) est fortement recommandée. Le chapitre Limiter les possibilités d'attaque avec Server Core de cet ouvrage couvre ce type d'installation. Le rôle Hyper-V est uniquement disponible dans la version 64 bits de Windows Server 2008.

La mémoire maximum est déterminée par le système d'exploitation. Windows Server 2008 édition standard permet 32 gigaoctets pour la partition racine et jusqu'à 31 gigaoctets par machine virtuelle.

Windows Server 2008 version entreprise et datacenter permettent un maximum de 1 Téra Octets pour la partition racine et jusqu'à 64 gigaoctets par machine virtuelle.

Il est recommandé d'avoir au moins deux cartes réseaux physiques (voir plus loin les meilleures pratiques). Chaque machine virtuelle peut avoir jusqu'à 12 cartes réseaux virtuelles (8 synthétiques + 4 émulées), chacune avec une adresse MAC statique ou dynamique. Les cartes réseaux synthétiques sont disponibles une fois les services d'invité virtuel installés et donc les pilotes adéquats. Les cartes réseaux émulées sont moins performantes. Elles utilisent un pilote standard qui ne nécessite pas les pilotes Hyper-V. Cela souligne l'importance de n'installer que des systèmes d'exploitation supportés par Hyper-V, afin d'avoir un réseau virtuel performant. La technologie vlan est supportée sur les cartes réseaux virtuelles. Un réseau virtuel ne peut pas être connecté à une carte réseau sans fil. Les machines virtuelles ne peuvent donc pas avoir de réseau sans fil.

Un lecteur de DVD virtuel peut utiliser des images ISO ou le lecteur physique du serveur. En revanche, une seule machine virtuelle peut accéder au lecteur physique en même temps. Il est donc recommandé de convertir les CD et DVD nécessaires en images ISO.

La configuration de plusieurs cartes réseaux en équipe (teaming) n'est actuellement pas supportée avec Hyper-V.

b. Méthodologie

La méthodologie est très importante dans un projet de virtualisation. Certains sujets comme la sauvegarde, doivent vraiment être traités avant le passage en production. Les phases classiques d'un projet d'infrastructure s'appliquent, avec quelques spécificités :

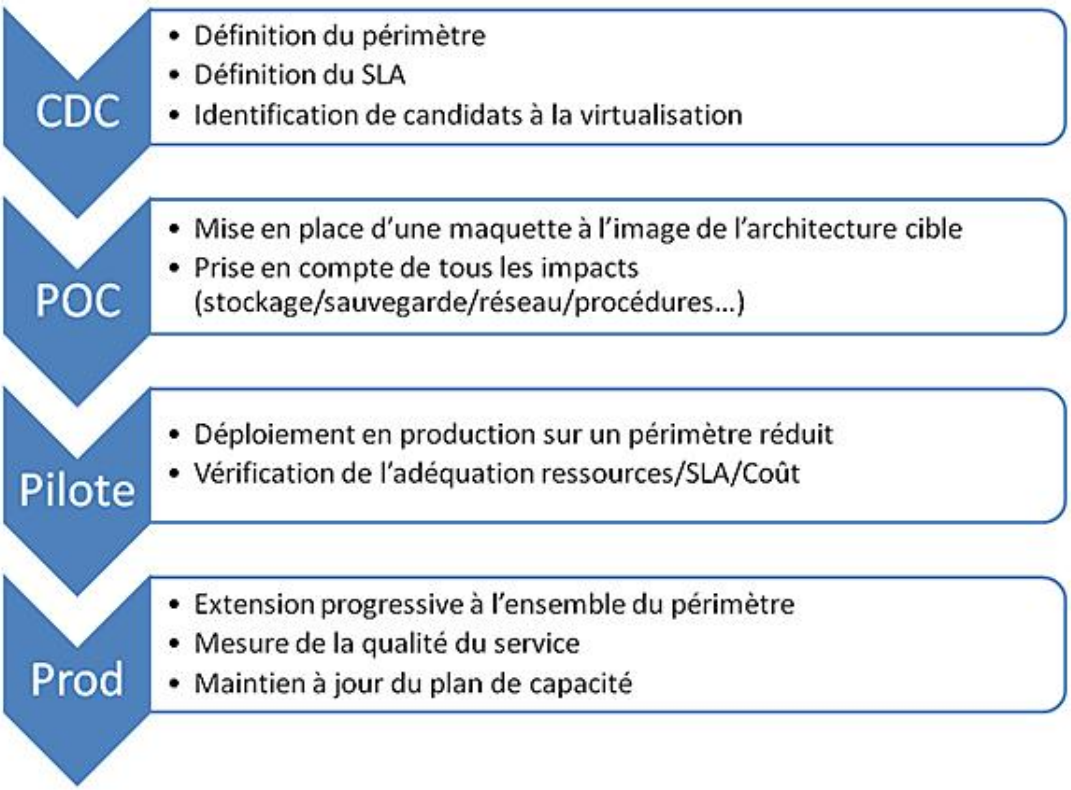
- Déterminer le périmètre (environnements, systèmes d'exploitation…).
- Commencer la chasse aux candidats à la virtualisation en implémentant des outils de mesures (voir la section suivante).
- Déterminer le niveau de service à fournir sur le périmètre (SLA).
- Monter une maquette/POC (*Proof Of Concept*).
    - Utiliser l'infrastructure de stockage pressentie (interne, SAN, ISCSI, partages de fichiers…).
    - Mesurer l'intégration dans l'architecture réseau existante (VLAN, filtrage par adresse mac, protection sur les commutateurs).
    - Implémenter au moins un exemplaire de chaque type de VM dans le périmètre (une VM de chaque OS et chaque application).
    - S'assurer de la capacité à sauvegarder et restaurer chacune de ces VM.

© ENI Editions - All rigths reserved

- Générer la même charge qu'en production avec les mêmes contraintes (traitements, fenêtre de sauvegarde…).
- Implémenter la solution de supervision en prenant en compte la virtualisation (mesurer l'utilisation des processeurs disponibles dans Hyper-V ainsi que la consommation par VM…).
- Évaluer l'intérêt de SCVMM dans votre contexte.
- Mesurer l'impact sur la gestion des mises à jour Windows (utilisation du « Offline servicing tool » plus bas).
- Mesurer l'impact sur les procédures d'exploitation (procédure d'arrêts/démarrages…).
- Évaluer l'impact sur les coûts.

- Mettre en place un pilote, qui sera la mise en production d'un échantillon du périmètre, afin de vérifier les hypothèses.
- Étendre le pilote à l'ensemble du périmètre, de façon progressive.

La maquette est décisive, car elle permet de lever toutes les nouveautés à venir et de vérifier que l'architecture pressentie tiendra la charge. Sous-évaluer cette phase risque de mener à l'échec une fois en production. La durée de cette phase doit permettre d'évaluer les impacts de la virtualisation, ainsi que les optimisations à mener, que ce soit sur Hyper-V, dans les machines virtuelles ou les autres briques du système d'information. Au terme de la maquette, tous les intervenants doivent avoir une vision claire des avantages et inconvénients de la virtualisation afin de pouvoir faire un bilan pertinent. Le pilote doit confirmer sans réserve ce bilan avant de généraliser le déploiement.


CDC
• Définition du périmètre
• Définition du SLA
• Identification de candidats à la virtualisation
POC
• Mise en place d'une maquette à l'image de l'architecture cible
• Prise en compte de tous les impacts (stockage/sauvegarde/réseau/procédures…)
Pilote
• Déploiement en production sur un périmètre réduit
• Vérification de l'adéquation ressources/SLA/Coût
Prod
• Extension progressive à l'ensemble du périmètre
• Mesure de la qualité du service
• Maintien à jour du plan de capacité

c. Déterminer les serveurs et applications propices à la virtualisation

Microsoft propose gratuitement un outil afin de préparer et accélérer votre projet de virtualisation : Microsoft Assessment and Planning Toolkit. Il est téléchargeable à cette adresse : http://www.microsoft.com/downloads/details.aspx?familyid=67240B76-3148-4E49-943D-4D9EA7F77730&displaylang=en

© ENI Editions - All rigths reserved

Vous pouvez ainsi très facilement :

- faire un inventaire des serveurs ;
- collecter les consommations de ressources sur ces serveurs ;
- générer des rapports Office sur les données collectées avec des recommandations.

Il est à installer de préférence sur un poste de travail, car il nécessite notamment Microsoft Office (2003 ou 2007), et une instance SQL Express. L'installation de ce dernier peut être évitée s'il est déjà présent, en créant au préalable une instance nommée « MAPS ».

Une fois installé, vous devrez :

- Créer une base pour le projet en cliquant sur **Select a database**.
- Créer manuellement un fichier texte contenant la liste des serveurs que vous souhaitez examiner pour votre projet de virtualisation (candidats potentiels). Par exemple, le script PowerShell suivant extrait le nom DNS de tous les serveurs de l'Active Directory dans le fichier **mondump.txt** :

```
$chercher = New-Object
DirectoryServices.DirectorySearcher("[ADSI]")
$chercher.SizeLimit = 10000
$chercher.PropertiesToLoad.Add("dNSHostName")
$chercher.Filter =
"(&(objectClass=Computer)(operatingSystem=*Serve*r*))"
$chercher.FindAll() | foreach-object
{$objet=$_.GetDirectoryEntry();$objet.dNSHostName;} >>
mondump.txt
```

- Cliquez sur **Capture performance metrics for server consolidation**.
- Indiquez le fichier texte créé précédemment.
- Spécifiez un ou plusieurs comptes ayant les droits administrateurs locaux sur les serveurs cibles.
- Spécifiez une date de fin pour la collecte des métriques. La station faisant la collecte doit rester opérationnelle tout le temps de la collecte.
- Vous pouvez ensuite générer les rapports.

d. Respect des meilleures pratiques

Voici quelques règles considérées comme des meilleures pratiques à respecter par défaut, sauf cas particulier.

De façon générale, sur Hyper-V :

- Prévoyez au moins deux cartes réseaux physiques sur le serveur :
  - une pour la gestion de l'hyperviseur,
  - une ou plusieurs dédiées aux machines virtuelles,
  - une ou plusieurs dédiées pour le ISCSI, si vous l'implémentez ;
- Connectez la carte réseau dédiée au management de l'hyperviseur sur votre réseau d'administration.
- N'exposez que les machines virtuelles au réseau Internet.

© ENI Editions - All rigths reserved

- Mettez une exclusion sur l'antivirus pour les fichiers *.vhd et *.avhd.

- Le lecteur DVD ne peut pas être partagé par plusieurs machines virtuelles. Privilégiez les images ISO à la place.

De façon générale, sur les machines virtuelles :

- Installez dès que possible les outils « services d'invité virtuel ».

- Désactivez l'économiseur d'écran.

- Défragmentez toujours le disque physique avant de créer un disque dur virtuel.

- Si vous migrez des machines virtuelles depuis d'autres solutions de virtualisation, comme Virtual PC, Virtual Server, VMware, désinstallez les « VMadditions » ou les « VMware Tools ». Compactez le disque dur virtuel avant de le déplacer sur Hyper-V.

- Assurez-vous que l'affichage est optimisé pour les performances, afin que l'accélération matérielle soit effective.

- Créez des disques virtuels de taille fixe. Les performances sont supérieures, le système de fichiers sera moins fragmenté, et la gestion de l'espace sera plus simple.

- Si vous créez une VM Windows Server 2003, attribuez-lui deux processeurs virtuels afin d'avoir un HAL multiprocesseur.

- Utilisez autant que possible les pilotes synthétiques une fois les services d'invité virtuel installés, afin d'augmenter les performances.

Vous pouvez avoir un contrôleur de domaine Active Directory à l'intérieur d'une machine virtuelle Hyper-V. Cependant les règles suivantes s'appliquent :

- N'utilisez jamais la sauvegarde d'état. Cela peut engendrer des erreurs de synchronisation si vous restaurez un état antérieur aux autres contrôleurs de domaine.

- Ne mettez pas en pause un contrôleur de domaine pour une longue période, cela peut impacter la réplication. Arrêtez plutôt la machine virtuelle si nécessaire.

- Ne faites pas d'images instantanées. Cette fonctionnalité n'est pas supportée par Microsoft dans le cas d'un contrôleur de domaine.

- Choisissez comment synchroniser le temps. Il est crucial que l'ensemble du domaine soit à la même heure. Par défaut, Kerberos ne supporte qu'un écart maximum de 5 minutes. Vous pouvez soit synchroniser sur l'horloge matérielle du serveur à travers les services d'invité virtuel, soit synchroniser via le réseau du domaine.

- Si votre seul contrôleur de domaine est une machine virtuelle dans Hyper-V, la partition racine (l'hyperviseur) ne doit pas être joint à ce domaine. Lorsque vous redémarrez le serveur, la partition racine cherchera un contrôleur de domaine qu'elle ne pourra pas trouver car la machine virtuelle ne sera pas encore démarrée.

Vous pouvez implémenter SQL Server dans une machine virtuelle. Dans ce cas, veuillez noter les remarques suivantes :

- Une machine virtuelle ne peut pas avoir plus de quatre processeurs virtuels. Votre charge SQL ne doit donc pas demander plus de quatre processeurs.

- Le stockage est un élément critique pour la base de données, et la virtualisation n'y change rien. Le stockage sur lequel résidera les données et journaux doit fournir les performances nécessaires. Afin de ne pas diminuer ces performances via la virtualisation, vous devriez utiliser uniquement des disques virtuels à taille fixe, en utilisant le pilote SCSI virtuel. L'autre alternative est l'utilisation de volumes directement en

© ENI Editions - All rigths reserved

pass-through.

Vous pouvez implémenter Exchange Server 2007 dans une machine virtuelle. Dans ce cas, veuillez noter les remarques suivantes :

- Afin que la configuration soit supportée par Microsoft, installez le Service Pack 1 pour Exchange 2007.
- L'utilisation de disques virtuels de taille dynamique n'est pas supportée.
- L'utilisation des fonctions d'images instantanées et différencielles sur les disques virtuels n'est pas supportée.

En ce qui concerne la sécurité, vous ne devriez jamais donner de droits sur la partition racine aux administrateurs de machines virtuelles. Afin de respecter le célèbre principe du moindre privilège, vous ne devez leur donner que le strict minimum nécessaire. Gérer cette sécurité peut devenir complexe, aussi vous pouvez utiliser la notion de rôles afin de classifier ces accès.

© ENI Editions - All rigths reserved

Déployer Hyper-V

1. Installation

L'installation est aussi simple que l'ajout du rôle sur le serveur. Si vous avez choisi une installation Core, exécutez la commande `start /wait ocsetup Microsoft-Hyper-V`, sinon exécutez la commande `servermanagercmd -i Microsoft-Hyper-V`.

Un redémarrage sera nécessaire pour prendre en compte le rôle. Vous avez intérêt à installer ces mises à jour complémentaires suivant les fonctionnalités que vous souhaitez utiliser. Voici une liste d'articles de KB pour Hyper-V :

N° d'article Microsoft	Description
KB950050	Améliore la sécurité, la stabilité, les performances, l'expérience utilisateur, la compatibilité ascendante des configurations et le modèle de programmation.
KB950792	Lorsque vous essayez d'activer, désactiver ou mettre à jour la technologie Hyper-V, le processus cesse de répondre.
KB954279	On ne vous demande pas d'informations d'identification après avoir reçu un « accès refusé » quand vous essayez de connecter une machine virtuelle depuis la MMC Hyper-V de Windows Server 2008.
KB954280	Message d'erreur lorsque vous essayez d'exporter une machine virtuelle sur un ordinateur Windows Server 2008 en fonction, qui utilise l'hyper-V: « une erreur lors de la tentative exporter l'ordinateur virtuel ».
KB954281	Après avoir installé Windows 2000 sur un ordinateur virtuel qui s'exécute dans un ordinateur Windows Server 2008 utilisant la technologie Hyper-V, vous pouvez créer un disque de démarrage de 127 Go au maximum.
KB954282	Le périphérique VMBus ne se charge pas sur un ordinateur virtuel qui est en cours d'exécution sur un ordinateur Windows Server 2008 avec Hyper-V.
KB954356	Après avoir déployé un Sysprep, le service de la couche Hyperviseur ne démarre pas automatiquement dans Windows Server 2008.
KB956589	Installez cette mise à jour pour résoudre d'éventuels problèmes lorsque vous gérez Hyper-V avec System Center Virtual Machine Manager (*SCVMM*).
KB956774	Un client de service de transfert intelligent en arrière-plan (BITS) ne peut pas gérer les fichiers qui ont des chemins d'accès qui contiennent le GUID dans Windows Server 2008 ou dans Windows Vista du volume.
KB956697	Installez cette mise à jour pour résoudre le problème suivant : le service de cliché instantané de volumes Hyper-V (VSS) ne sauvegarde pas correctement les ordinateurs virtuels.
KB956710	Installez cette mise à jour pour améliorer la prise en charge par le rôle Hyper-V des processeurs et ordinateurs virtuels pour prendre en charge jusqu'à 24 processeurs logiques et 192 ordinateurs virtuels.
KB951308	La page n'existe pas en français. Increased functionality and virtual machine control in the Windows Server 2008 Failover Cluster Management console for the Hyper-V role.
KB953828	L'hôte équilibrage de charge réseau ne converge comme prévu sur les ordinateurs virtuels Windows Server 2008 Hyper-V.
KB953585	Message d'erreur lorsque vous essayez de démarrer un ordinateur virtuel Hyper-V sur un ordinateur Windows Server 2008 ou Windows Vista qui utilise l'architecture NUMA : « une

© ENI Editions - All rigths reserved

	erreur lors de la tentative modifier l'état de machine virtuelle VMNAME ».
KB950182	Un ordinateur qui exécute une version x86 - version de Windows Server 2008 ou Windows Vista qui peut utiliser moins de processeurs que prévu si le nombre de cœurs sur un socket n'est pas une puissance de 2.
KB957967	Message d'erreur d'arrêt sur un ordinateur Windows Server 2008 qui possède le rôle hyper-V installé : « Stop 0x0000001A ».
KB958065	Vous ne pouvez pas configurer une machine virtuelle sous technologie Hyper-V à l'aide de la gestion des clusters Windows Server 2008 lorsque la machine virtuelle utilise un périphérique de stockage géré par un système de fichiers en cluster tiers ou une solution de réplication tiers.
KB958184	Les opérations de sauvegarde des machines virtuelles échouent dans Windows Server 2008 lorsque les fichiers des machines virtuelles Hyper-V sont enregistrés sur un volume qui est monté sur un cluster avec basculement en utilisant un GUID du volume.
KB958665	Vous ne recevez pas un message d'erreur après avoir restauré une machine virtuelle Windows Server 2008 sous Hyper-V.
KB958668	Vous ne pouvez pas arrêter une machine Windows 2000 SP4 verrouillée dans le Gestionnaire Hyper-V sur un serveur qui exécute Windows Server 2008.
KB958829	La page n'existe pas en français. When Hyper-V is installed in SBS 2008 it causes the bindings for DHCP to bind to the incorrect interface.
KB959781	La page n'existe pas en français Windows 2000 with Integration Services may shut down slowly while running as a guest on Server 2008 with Hyper-V.
KB959978	Message d'erreur lorsque vous sauvegardez un ordinateur virtuel Windows Server 2003 dans Hyper-V : « GetWriterStatus a échoué pour l'enregistreur sélectionné [Enregistreur VSS de Microsoft Hyper-V], enregistreur est dans l'état [9] [VSS_WS_FAILED_AT_FREEZE] ».
KB960024	La page n'existe pas en français. Error message when you try to create a new virtual machine in Windows Vista or Windows Server 2008: "The Encountered an Error while creating a Virtual Machine".
KB960038	Vous recevez un stop 0x0000007E sur des ordinateurs hôtes Hyper-V Windows Server 2008 lorsque vous utilisez l'enregistreur de la technologie Hyper-V pour sauvegarder des ordinateurs virtuels.

Sur une installation Core, vous devez télécharger ces mises à jour depuis une autre machine qui a un navigateur Internet. Vous devez ensuite les copier sur le serveur, et les installer avec la commande suivante :

```
wusa.exe nom_du_fichier.msu /quiet
```

L'état d'installation des mises à jour Windows, que ce soit par l'installation manuelle ou le client Windows update, peut être vérifié en regardant les journaux d'évènements. Pour la version Core, la commande suivante les affiche sur la console :

```
wevtutil qe System /q:"*[System[Provider[@Name='Microsoft-
Windows-WindowsUpdateClient']]]" /f:Text
```

2. Configuration du rôle

La configuration du rôle couvre différents aspects :

- création et configuration des réseaux virtuels ;

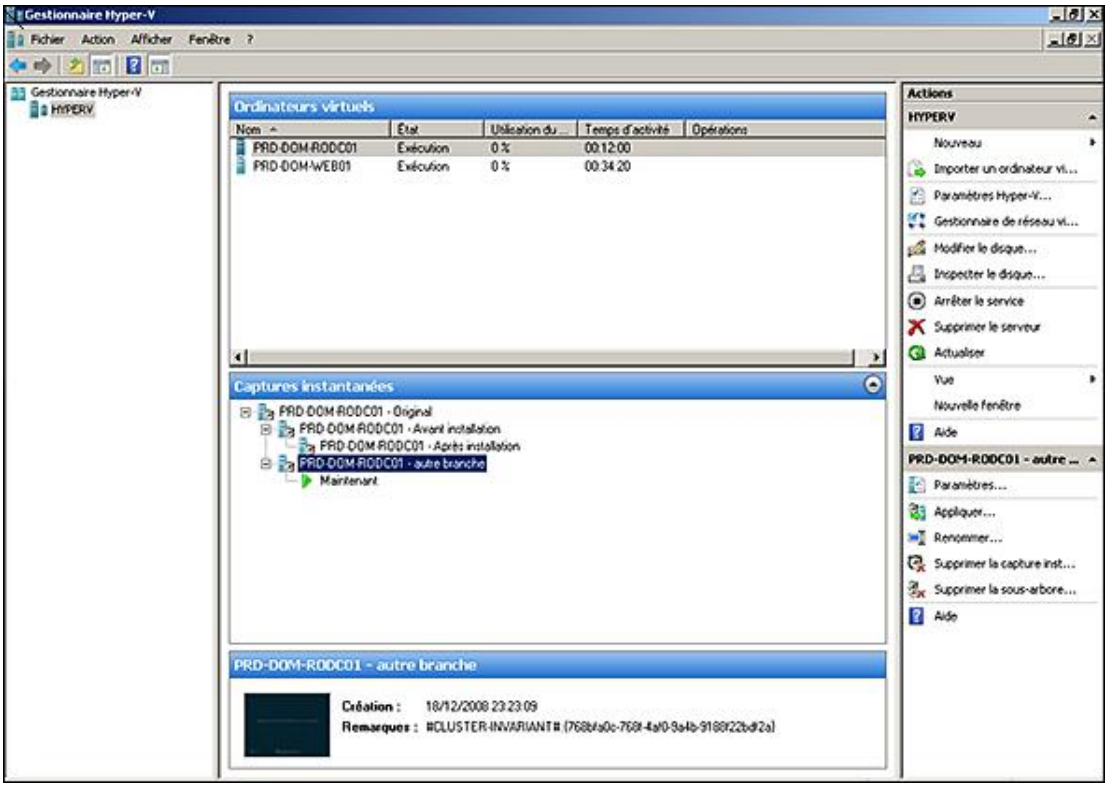
© ENI Editions - All rigths reserved

- mise à disposition d'images iso pour les différentes installations.

La console de gestion Hyper-V est disponible à la fois en 32 et 64 bits, pour Windows Server 2008 et Windows Vista. Une mise à jour est disponible pour cette console :

```
Mise à jour relative à la gestion à distance de Hyper-V pour
Windows Vista pour ordinateurs à processeur x64 (KB952627)
http://support.microsoft.com/kb/952627
```

La console permet de gérer les serveurs Hyper-V ainsi que les machines virtuelles qu'ils hébergent. Ouvrez la console **Gestionnaire Hyper-V** en cliquant sur le bouton **Démarrer**, **Outils d'administration** puis **Gestionnaire Hyper-V**.



3. Configuration du stockage

Le stockage est le nerf de la guerre avec la virtualisation. Cela est d'autant plus vrai si les services offerts dans les machines virtuelles sont elles aussi consommatrices en entrées/sorties disques. Afin de réduire les coûts, il est intéressant d'utiliser du stockage « low cost », mais le risque est d'avoir des lenteurs certaines dans les machines virtuelles. Il vous faut donc trouver le juste équilibre, entre une solution SAN et un partage réseau ! Hyper-V supporte un large panel de solutions pour le stockage des machines virtuelles :

- Stockage local au serveur (IDE/SATA/ESATA/USB/Firewire/SAS/SCSI) ;
- Stockage sur un SAN ;
- Stockage via ISCSI ;
- Stockage sur un partage de fichiers ;
- Stockage en pass-through.

Vous pouvez même stocker les VM sur une clé USB, moyennant qu'elle soit formatée en NTFS. Par défaut, vous devriez utiliser des disques virtuels. Il y a cependant certains cas où vous devrez utiliser un stockage en pass-through. Cette méthode donne un accès direct à la VM à une zone de stockage, comme si c'était une machine physique. Un des avantages est une meilleure performance, liée à l'absence de la couche de virtualisation. Voici quelques considérations à propos du mode pass-through :

© ENI Editions - All rigths reserved

- Les disques virtuels ont une limite de 2 teraoctets. L'accès en pass-through permet de lever cette limite jusqu'au maximum supporté par le système d'exploitation.

- Les volumes en pass-through ne sont pas sauvegardés par les mécanismes Hyper-V. Il vous faudra les sauvegarder par un autre moyen.

- Les mécanismes d'images instantanées ne sont pas disponibles sur ce type de volume.

Si vous choisissez de stocker les VM sur un partage de fichiers, il est recommandé de rendre ce partage hautement disponible. Le stockage via ISCSI peut se faire de deux manières : depuis la partition racine, ou depuis la machine virtuelle. Ce choix a plusieurs conséquences :

- Si le stockage ISCSI est accédé depuis la partition racine, les performances sont meilleures que depuis la VM, et la sauvegarde via l'enregistreur VSS est supportée.

- Les machines virtuelles ne peuvent pas être démarrées depuis un stockage ISCSI (géré depuis les VM au lieu de la partition racine). Le stockage ISCSI accédé depuis la VM ne peut pas être sauvegardé via le VSS Hyper-V.

Un autre choix à faire porte sur la nature des contrôleurs virtuels pour les machines virtuelles. Ils peuvent être IDE ou SCSI. L'aspect performance ne joue pas du moment que les services d'invité virtuel sont installés. Les différences portent sur la volumétrie et le nombre de disques virtuels attachés à la VM. Le contrôleur SCSI ne permet pas de démarrer la VM, mais permet jusqu'à 256 périphériques de stockage (4 contrôleurs * 64 périphériques). Les volumes rattachés au contrôleur IDE sont au maximum 4 (en comptant le lecteur CD/DVD virtuel), et ont une taille maximum de 128 gigaoctets.

Le stockage sur une infrastructure SAN est généralement la plus performante, et aussi la plus coûteuse. La technologie NPIV est disponible sur les cartes HBA, ce qui permet de respecter les meilleures pratiques pour le stockage SAN (zoning…). Vous devez pour cela activer les WWN (*World Wide Names*) virtuels pour les machines virtuelles. Voici quelques considérations pour le stockage sur un SAN :

- Un pilote MPIO (multiport) est nécessaire, même avec une seule HBA.

- Désactivez le montage automatique des volumes.

- Laissez les disques en basiques.

- Tous les fichiers de VM doivent être sur un seul volume.

- Ajoutez les LUN en tant que ressource disque au cluster avant de créer les VM.

Si les VM sont stockées en pass-through sur le SAN, deux LUN sont requises, une pour le disque de démarrage et une pour la configuration.

4. SCVMM 2008

L'installation du module complémentaire SCVMM (*System Center Virtual Machine Manager*) 2008 est simple et rapide. Il ne faut pas pour autant sous-estimer son apport fonctionnel dans la gestion de l'infrastructure. Les fonctionnalités principales sont :

- Centralisation du déploiement et de la gestion des machines virtuelles pour Hyper-V, Virtual Server et VMware ESX.

- Conversion P2P et P2V rapide et fiable, sans outil supplémentaire.

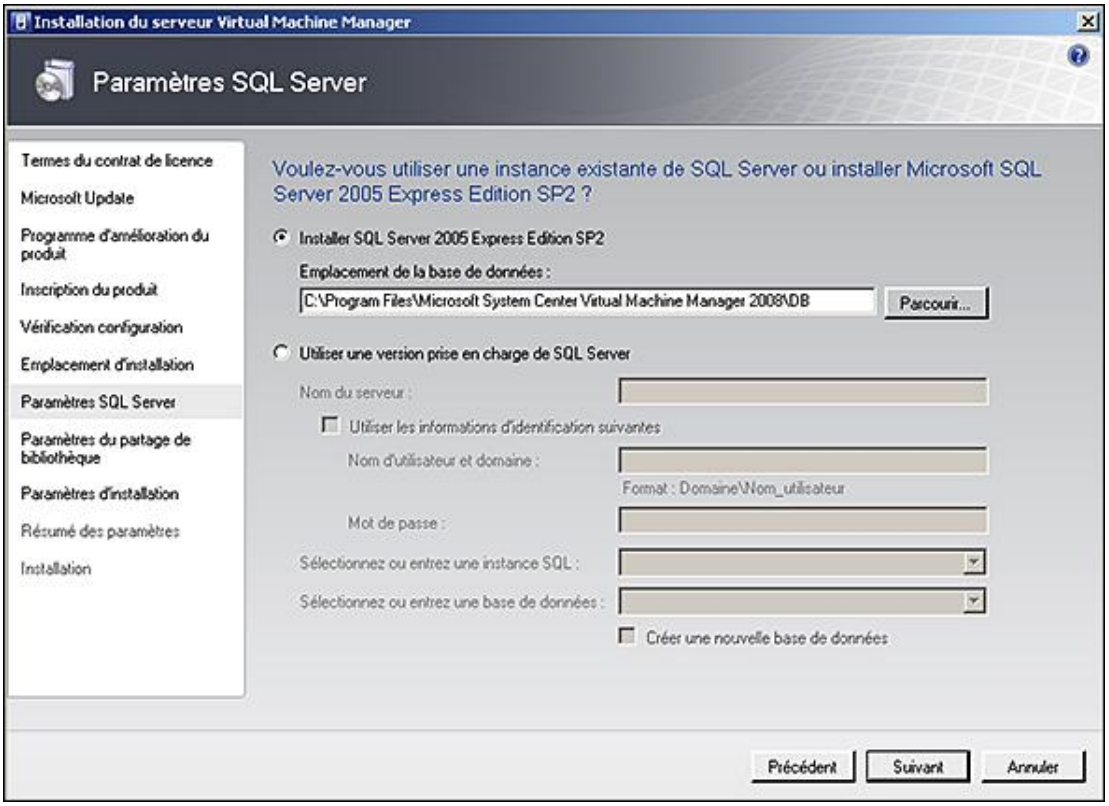
- Intégration avec SCOM pour la supervision.

- Optimisation des ressources et de la performance en proposant des déplacements et placements de machines virtuelles.

© ENI Editions - All rigths reserved

- Gestion centrale d'une bibliothèque de composants pour les machines virtuelles.
- Délégation de certaines tâches d'administration.
- Portail libre service pour la génération de machines virtuelles.
- Intégration avec le cluster Windows Server 2008 (failover).
- Entièrement scriptable à travers PowerShell.
- Génération de rapports sur l'état de l'infrastructure virtuelle.

Il n'est cependant pas possible de l'installer sur une installation Core de Windows Server 2008. Le seul choix réel à faire pendant l'installation concerne la base de données de SCVMM 2008. Vous pouvez soit utiliser un moteur SQL Express 2005, soit lui indiquer un serveur SQL 2005 existant :


Installation du serveur Virtual Machine Manager
Paramètres SQL Server
Termes du contrat de licence
Microsoft Update
Programme d'amélioration du produit
Inscription du produit
Vérification configuration
Emplacement d'installation
Paramètres SQL Server
Paramètres du partage de bibliothèque
Paramètres d'installation
Résumé des paramètres
Installation
Voulez-vous utiliser une instance existante de SQL Server ou installer Microsoft SQL Server 2005 Express Edition SP2 ?
Installer SQL Server 2005 Express Edition SP2
Emplacement de la base de données :
C:\Program Files\Microsoft System Center Virtual Machine Manager 2008\DB
Parcourir...
Utiliser une version prise en charge de SQL Server
Nom du serveur :
Utiliser les informations d'identification suivantes
Nom d'utilisateur et domaine :
Format : Domaine\Nom_utilisateur
Mot de passe :
Sélectionnez ou entrez une instance SQL :
Sélectionnez ou entrez une base de données :
Créer une nouvelle base de données
Précédent
Suivant
Annuler

Après l'installation de SCVMM 2008, il faut démarrer manuellement son service Windows si vous ne souhaitez pas redémarrer le serveur. Vous avez deux possibilités pour gérer votre environnement virtuel avec SCVMM :

- via son interface graphique ;
- via l'extension PowerShell.

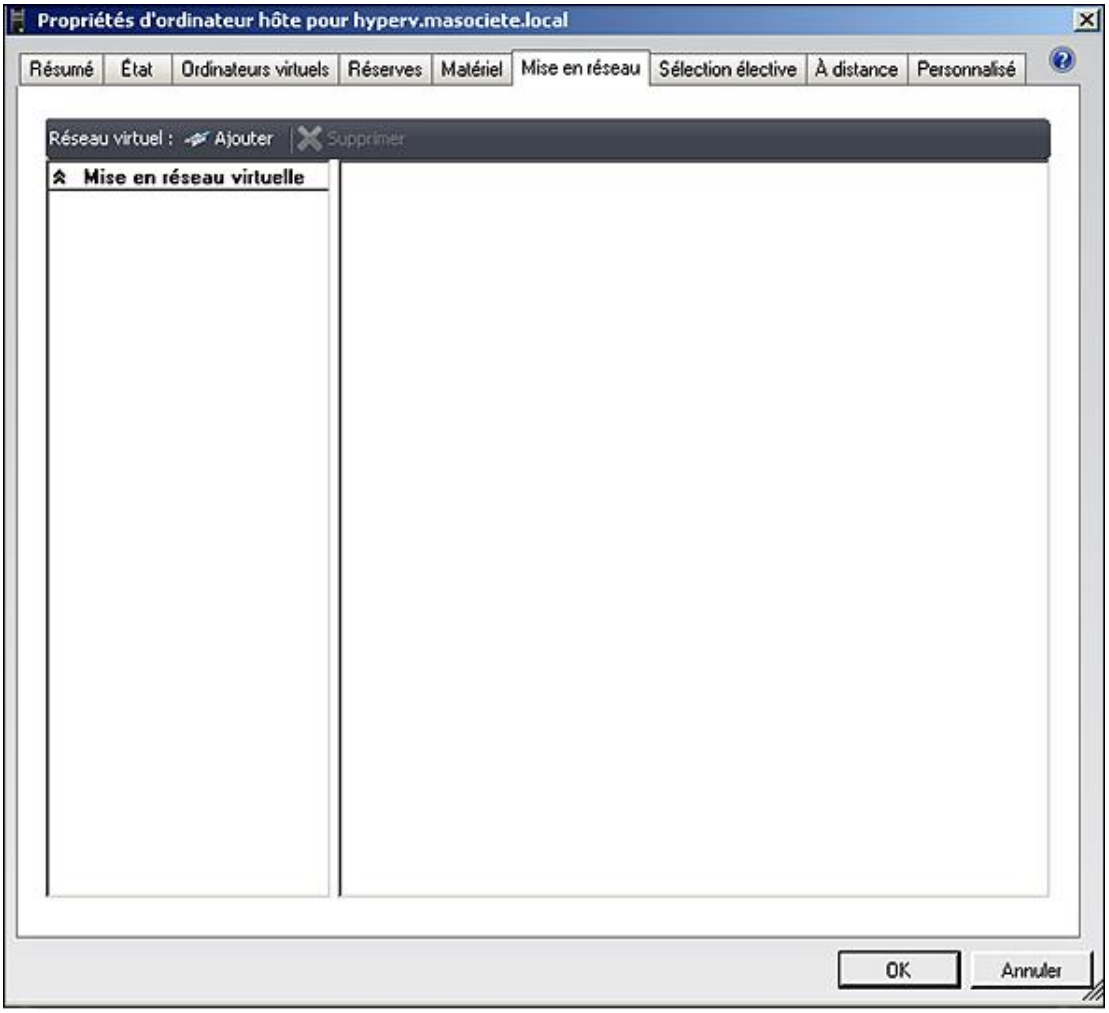
Avant de provisionner les machines virtuelles, vous devriez :

- Déclarer les serveurs Hyper-V à gérer (au moins un).
- Déclarer les réseaux virtuels.
- Créer des modèles de profils pour les machines virtuelles.
- Ajouter les images ISO à la bibliothèque.

© ENI Editions - All rigths reserved

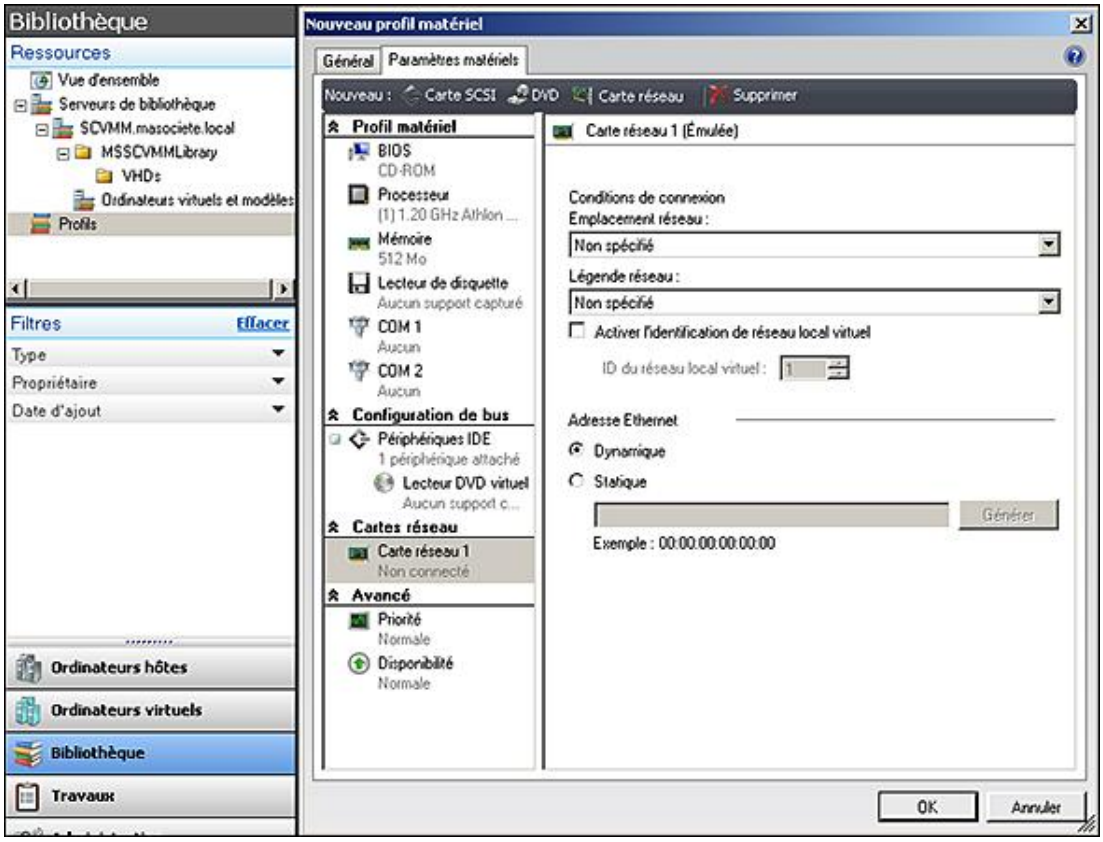
- Créer des modèles de disques virtuels.

La déclaration de réseaux virtuels se fait depuis les propriétés du serveur virtuel :



Les profils matériels permettent d'utiliser des modèles de configuration plutôt que de configurer manuellement les ressources à chaque ajout de VM. Au-delà du gain en efficacité lors la création de VM, cela permet d'avoir une consistance de configuration entre deux machines virtuelles, gage de qualité. Pour gérer les profils matériels, allez dans **bibliothèque**, puis **Profils**. Un profil comprend les paramètres suivants :

© ENI Editions - All rigths reserved



L'ajout d'image ISO consiste simplement à copier les fichiers ISO dans le partage de la bibliothèque SCVMM.

Lors d'une actualisation de la bibliothèque, Virtual Machine Manager indexe les fichiers enregistrés sur les partages de bibliothèque, puis met à jour la vue **Bibliothèque** et la liste de ressources. Tous les fichiers ne sont pas indexés et tous les fichiers indexés n'apparaissent pas dans la vue Bibliothèque. Le contenu de la bibliothèque est automatiquement rafraîchit toutes les heures par défaut. Le type de contenu suivant est indexé :

- les disques durs virtuels : .vhd (Hyper-V, Virtual Server), .vmdk (VMware) ;
- les disquettes virtuelles : .vfd (Virtual Server), .flp (VMware) ;
- les images ISO : .iso ;
- les fichiers de réponses : .ps1 (Windows PowerShell) ; .inf ou .xml ;
- les modèles VMware : .vmtx.

Les types de fichiers de configuration suivants sont indexés, mais ils ne sont pas ajoutés à la bibliothèque en tant que ressources :

- Hyper-V : .exp (format d'exportation), .vsv (état enregistré), .bin ;
- Virtual Server : .vmc (configuration de l'ordinateur virtuel), .vsv (état enregistré) ;
- VMware : .vmtx (configuration de l'ordinateur virtuel), .vmx (format d'exportation) ;
- Les disques durs virtuels, images ISO et disquettes virtuelles attachés à un ordinateur virtuel.

La gestion des machines virtuelles peut se faire en PowerShell, ce qui ouvre les portes nécessaires aux planifications, automatisations et traitements de masses.

Voici quelques exemples de commandes PowerShell :

#Récupération du compte d'accès :

© ENI Editions - All rigths reserved

```
$Credential = get-credential
```

#Récupération de l'identifiant du groupe "Tous les ordinateurs hôtes" :

```
$VMHostGroup = Get-VMHostGroup -VMMServer localhost | where
{$_.Path -eq "Tous les ordinateurs hôtes"}
```

#Ajout de la ressource Hyper-V :

```
Add-VMHost -VMMServer localhost -ComputerName
"hyperv.masociete.local" -Description "" -Credential
$Credential -RemoteConnectEnabled $true -VmPaths " E:\VMDATA"
-Reassociate $false -RunAsynchronously -RemoteConnectPort
2179 -VMHostGroup $VMHostGroup
```

#Déclaration d'un nouvel adaptateur réseau virtuel :

```
New-VirtualNetworkAdapter -VMMServer localhost -JobGroup
e4c2dfd1-0091-4a2a-992f-3406cfe833eb -PhysicalAddressType
Dynamic -VirtualNetwork "Net_LAN" -VLanEnabled $false
```

#Déclaration d'un nouveau lecteur DVD Virtuel :

```
New-VirtualDVDDrive -VMMServer localhost -JobGroup e4c2dfd1-
0091-4a2a-992f-3406cfe833eb -Bus 1 -LUN 0
```

#Utilisation d'un type de processeur déjà existant :

```
$CPUType = Get-CPUType -VMMServer localhost | where {$_.Name
-eq "3.07 GHz Xeon"}
```

#Déclaration d'un nouveau profil matériel pour les VM :

```
New-HardwareProfile -VMMServer localhost -Owner
"MASOCIETE\mchateau" -CPUType $CPUType -Name
"Profil11d45f28-11b9-414b-aca0-ce8fbf6b9081" -
Description "Configuration matérielle utilisée pour
créer un ordinateur virtuel/modèle" -CPUCount 2 -
MemoryMB 512 -RelativeWeight 100 -HighlyAvailable $false -
NumLock $false -BootOrder "CD", "IdeHardDrive",
"PxeBoot", "Floppy" -LimitCPUFunctionality $false -
JobGroup e4c2dfd1-0091-4a2a-992f-3406cfe833eb
```

#Récupération d'un profil matériel existant :

```
$HardwareProfile = Get-HardwareProfile -VMMServer
localhost | where {$_.Name -eq "Profil11d45f28-11b9-
414b-aca0-ce8fbf6b9081"}
```

#Déclaration d'un nouveau disque virtuel :

```
New-VirtualDiskDrive -VMMServer localhost -IDE -Bus 0 -
LUN 0 -JobGroup e4c2dfd1-0091-4a2a-992f-3406cfe833eb -
Size 40960 -Dynamic -Filename "PRD-DOM-WEB01_disque_1"
```

#Récupération d'un système d'exploitation existant :

```
$OperatingSystem = Get-OperatingSystem -VMMServer
localhost | where {$_.Name -eq "64-bit edition of
Windows Server 2008 Standard"}
```

#Récupération d'un serveur Hyper-V :

```
$VMHost = Get-VMHost -VMMServer localhost | where
{$_.Name -eq "hyperv.masociete.local"}
```

#Déclaration d'une nouvelle machine virtuelle :

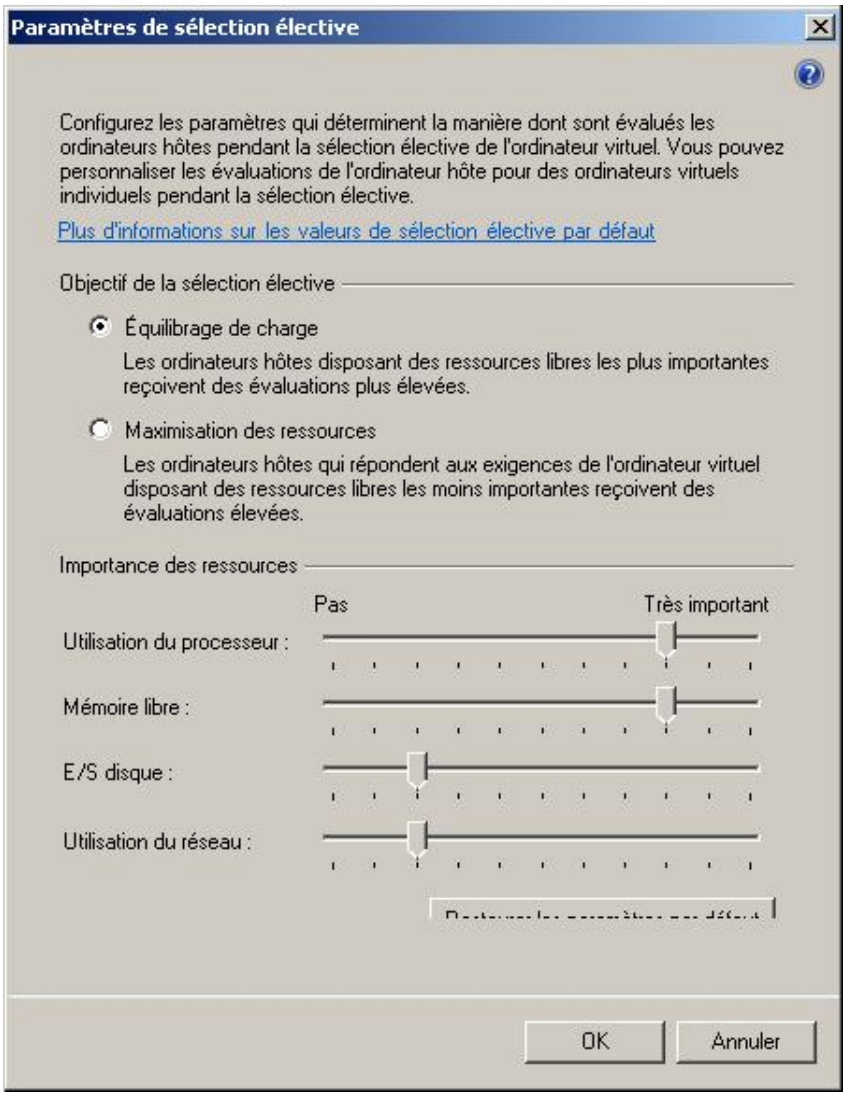
© ENI Editions - All rigths reserved

```
New-VM -VMMServer localhost -Name "PRD-DOM-WEB01" -
Description "Serveur WEB IIS sur le domaine" -Owner
"MASOCIETE\mchateau" -VMHost $VMHost -Path "E:\VMDATA" -
HardwareProfile $HardwareProfile -JobGroup e4c2dfd1-
0091-4a2a-992f-3406cfe833eb -RunAsynchronously -
OperatingSystem $OperatingSystem -RunAsSystem -
StartAction TurnOnVMIfRunningWhenVSStopped -DelayStart 0
-StopAction ShutdownGuestOS
```

Si vous souhaitez gérer des clusters Hyper-V depuis SCVMM, voici quelques considérations :

- Si vous ajoutez du stockage sur un cluster et souhaitez immédiatement ajouter des machines virtuelles sur ce stockage, assurez-vous au préalable que le cluster a été rafraîchi dans SCVMM pour prendre en compte ce nouveau stockage.
- La création/suppression des clusters ne peut pas être faite dans SCVMM.
- Les clusters qui ne sont pas dans un domaine de confiance ne peuvent pas être gérés par SCVMM.

L'optimisation des ressources peut être gérée en fonction des paramètres suivants :


Paramètres de sélection élective
Configurez les paramètres qui déterminent la manière dont sont évalués les ordinateurs hôtes pendant la sélection élective de l'ordinateur virtuel. Vous pouvez personnaliser les évaluations de l'ordinateur hôte pour des ordinateurs virtuels individuels pendant la sélection élective.
Plus d'informations sur les valeurs de sélection élective par défaut
Objectif de la sélection élective
Équilibrage de charge
Les ordinateurs hôtes disposant des ressources libres les plus importantes reçoivent des évaluations plus élevées.
Maximisation des ressources
Les ordinateurs hôtes qui répondent aux exigences de l'ordinateur virtuel disposant des ressources libres les moins importantes reçoivent des évaluations élevées.
Importance des ressources
Pas
Très important
Utilisation du processeur :
Mémoire libre :
E/S disque :
Utilisation du réseau :
OK
Annuler

Cet ensemble de critères est ensuite utilisé pour suggérer les placements et déplacements des machines virtuelles à travers une notation étoilée.

SCVMM permet également de gérer l'attribution des adresses MAC aux machines virtuelles. Par défaut, une plage est positionnée, mais elle peut être changée en cas de problèmes :

© ENI Editions - All rigths reserved

Administration
Mise en réseau
Mise en réseau (1)
Administration
Vue d'ensemble
Général
Ordinateurs gérés
Mise en réseau
Rôles d'utilisateurs
System Center
Gestionnaires de virtualisation
Rechercher
Aucun
Nom
Plage d'adresses globales statiques MAC
Plage d'adresses globales statiques MAC
Configurez la plage statique des adresses MAC que VMM doit utiliser lors de la création de nouveaux périphériques réseau virtuels pour des ordinateurs virtuels nouveaux ou existants. Lorsqu'une adresse MAC de la liste a été utilisée, elle ne sera plus jamais réutilisée par VMM.
En savoir plus sur les plages d'adresses MAC
Plage d'adresses MAC
Plage de début à :
00-1D-D8-B7-1C-00
Plage de fin à :
00-1D-D8-F4-1F-FF
OK
Annuler

5. Mises à jour Windows

Afin de faciliter l'installation des mises à jour Windows, Microsoft propose un outil complémentaire à SCVMM, « Offline Virtual Machine Servicing Tool 2.0 ». L'objectif de cet outil est de démarrer les machines virtuelles sur un réseau isolé (de préférence), déclencher les mises à jour Windows, et éteindre la machine virtuelle, en la mettant de nouveau dans la librairie. Il nécessite d'une part SCVMM, et d'autre part un serveur WSUS local (gratuit) ou SCCM. Il peut être téléchargé à cette adresse :

http://www.microsoft.com/downloads/details.aspx?FamilyId=8408ECF5-7AFE-47EC-A697-EB433027DF73&displaylang=en

---

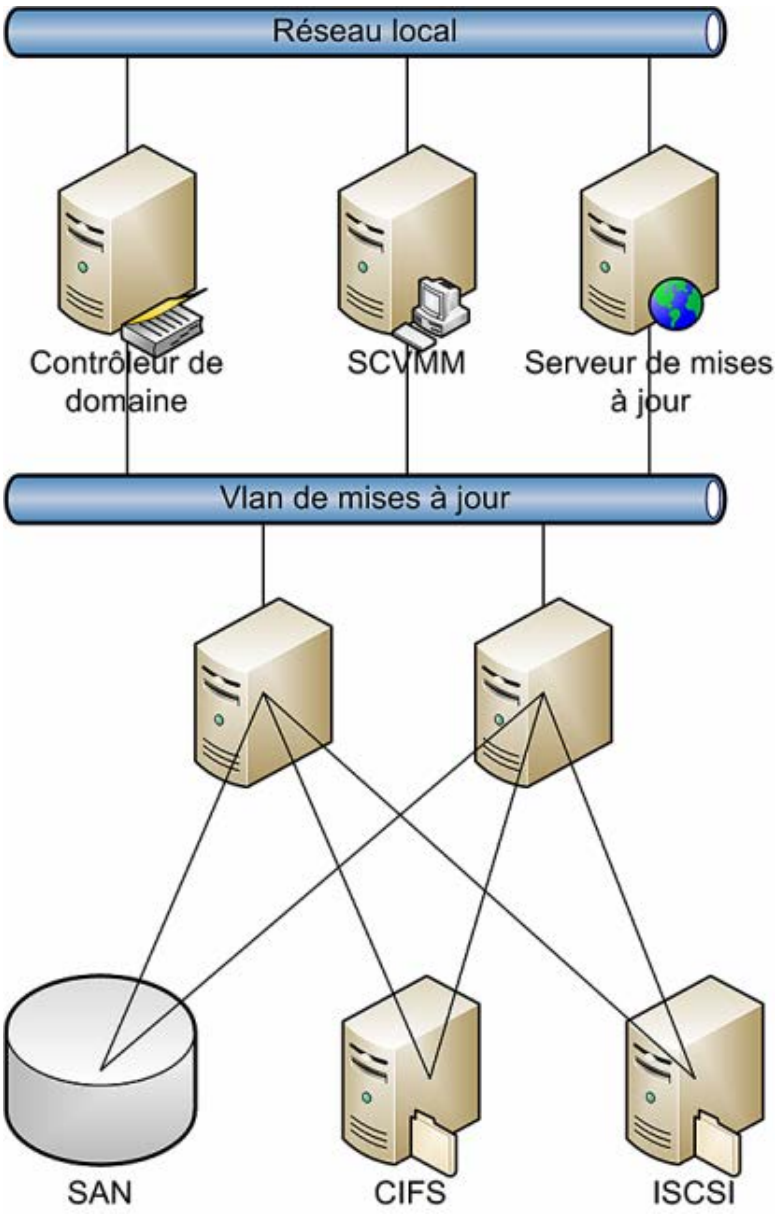
Cet outil est proposé à la fois en 32 et en 64 bits.

Il est recommandé pour les infrastructures virtuelles conséquentes, ayant un nombre important de machines virtuelles arrêtées, ou pour des environnements où la sécurité est un facteur important. Avant de décider d'utiliser cet outil ou non, voici quelques considérations à prendre en compte :

- Les VM doivent être configurées pour utiliser le serveur WSUS via GPO ou autre (non pris en charge par l'outil), ou avoir le client SCCM installé et configuré.
- WSUS ou SCCM doit être configuré au préalable afin que les mises à jour soient déjà approuvées pour déploiement sur ces VM.
- Les VM doivent être en DHCP, ou avoir une configuration réseau fonctionnelle dans le réseau de mises à jour.
- Si plus de 20 machines virtuelles sont à maintenir à jour avec l'outil, il est recommandé que l'infrastructure autour soit physique et non virtuelle (serveurs WSUS, SCVMM…).
- Il fonctionne à la fois sur une infrastructure Hyper-V et Virtual Server 2005.
- Tous les serveurs physiques et machines virtuelles doivent faire partie du domaine Active Directory, avec le service DNS en place et configuré.

Voici un exemple d'architecture :

© ENI Editions - All rigths reserved



© ENI Editions - All rigths reserved

Windows 2008 R2

Le rôle Hyper-V ne manque pas de nouveautés avec Windows Server 2008 R2. Les nouvelles fonctionnalités seront :

- Migration à chaud des machines virtuelles ;
- Hyper-V 2.0 ;
- Mise en veille des cœurs non utilisés ;
- Ajout et suppression de stockage dans les VM à chaud (sans redémarrage) ;
- Support pour les CSV (*Clustered Shared Volumes*) ;
- Synchronisation des interruptions entre VM ;
- Implémentation du SLAT Intel et AMD ;
- D'un point de vue réseau :
    - Support du TCP offload,
    - Support de la technologie VMQ (*Virtual Machine Queue*),
    - Support des « jumbo frames ».

La migration à chaud (live migration) permet de déplacer une machine virtuelle d'un serveur à l'autre sans perte de service (perte de connexion réseau). Pour ce faire, plusieurs étapes sont nécessaires :

- Création de la VM sur la cible.
- Copie des pages mémoires depuis la source vers la destination. Les pages modifiées pendant le transfert sont envoyées de nouveau (marquées « dirty »), jusqu'à 10 fois.
- La machine virtuelle est mise en pause sur la source.
- L'accès au stockage (le disque virtuel de la VM) est donné au serveur cible.
- La machine virtuelle est remise en fonctionnement.

Le Clustered Shared Volume permet à plusieurs serveurs d'accéder aux fichiers à l'intérieur d'une LUN. Un nœud est propriétaire de l'espace de noms et reste un passage obligé pour la création/suppression de meta données (répertoires…). Cependant, différents nœuds peuvent accéder à différents fichiers sur cette LUN en simultané, notamment les fichiers VHD. Cela permet donc de stocker tous les fichiers VHD sur une seule LUN. Tous les nœuds pouvant accéder à l'ensemble des fichiers, il n'est plus nécessaire de changer le propriétaire de la LUN.

Les LUN peuvent aussi être changées de propriétaire sans interruption, car les descripteurs sont persistants.

Avant Windows Server 2008 R2, chaque machine virtuelle a sa propre cadence d'interruptions. Cela cause une surcharge de travail pour l'hyperviseur, même quand les machines virtuelles n'ont pas d'activité. Afin de réduire cette surcharge, R2 implémente une synchronisation des interruptions entre machines virtuelles, en utilisant un multiple de l'interruption du serveur. Du point de vue des machines virtuelles, le moment où démarre la première interruption n'a pas d'impact, du moment qu'ensuite l'interruption arrive tout le temps à la même fréquence.

Intel et AMD proposent de décharger les hyperviseurs de la gestion de second niveau des adresses en mémoire (SLAT - *Second Level Address Translation*). Intel nomme cette technologie EPT (*Extended Page Tables*) et NPT (Nested Page Tables) ou RVI (*Rapid Virtualization Indexing*) chez AMD. Cela devrait permettre d'économiser environ 2 % de processeurs et 1Mo de mémoire par machine virtuelle.

La technologie VMQ permet à la carte réseau d'envoyer directement les paquets réseaux dans l'espace tampon en mémoire de la VM, sans passer par la partition racine. Cela évite aussi de vérifier le routage dans les switch virtuels via

© ENI Editions - All rigths reserved

les VMQ Queue ID. L'objectif est un gain de performance en réduisant le nombre d'opérations à faire pour les communications réseaux.

Le TCP Offload permet de décharger la gestion du trafic TCP/IP des machines virtuelles sur une carte physique du serveur. Ce déchargement augmente les performances et réduit la consommation processeur du serveur physique. La migration à chaud de VM peut tirer parti de cette fonctionnalité.

L'utilisation de « jumbo frames » permet de réduire le nombre de paquets par seconde à traiter en utilisant des trames de 9014 octets. Cela réduit notamment le nombre d'interruption par seconde sur les cartes réseaux, tout en augmentant le débit. Il est à noter que les équipements réseaux (commutateurs…) doivent supporter également les « jumbo frames ».

En conclusion, vous connaissez maintenant ce que peux vous apporter la virtualisation, moyennant de prendre en compte ses spécificités. Si comme de plus en plus d'administrateurs, vous voyez un net avantage à virtualiser, vous devriez faire une maquette afin de valider vos hypothèses. Suivant votre contexte, la complexité de ce type de projet peut fortement varier, et doit donc être préparé en conséquence. Comme indiqué en introduction, pensez grand mais commencez petit, afin d'avoir une montée en charge maîtrisée. L'édition R2 permettra de répondre à encore plus d'exigences, notamment avec la fonctionnalité « Live Migration » tant attendue.

© ENI Editions - All rigths reserved

Introduction

Ce chapitre a pour but de vous permettre d'aborder la sécurité de votre architecture de la meilleure des façons. En effet, il n'est pas rare d'entendre les professionnels de l'informatique s'exprimer avec des idées assez arrêtées en terme de sécurité. Ce domaine évoluant très régulièrement et très vite, il ne serait pas raisonnable de penser que l'architecture informatique et les solutions en terme de sécurité sont à jour. Il convient de se tenir régulièrement informé et de respecter un ensemble de bonnes pratiques.

Ce chapitre a donc pour intérêt de lister ces différentes bonnes pratiques et de vous présenter les nouvelles fonctionnalités vous permettant de les mettre en œuvre.

© ENI Editions - All rigths reserved

Principe de moindre privilège

Le principe de moindre privilège est, comme son nom l'indique, un principe qui consiste à lancer chaque tâche avec un compte utilisateur qui a exactement les permissions nécessaires à l'accomplissement de cette tâche.

Dans la pratique cela n'est bien sûr pas toujours réalisable mais il convient de toujours faire au mieux afin d'être le plus proche du besoin tout en laissant une surface d'attaque la plus réduite possible. Si un utilisateur n'a pas besoin de droits spécifiques pourquoi les lui fournir ? Et comment s'assurer que l'utilisateur n'a pas plus de droits qu'il ne lui en faut ?

Différentes notions techniques sont à connaître afin de pouvoir faire les meilleurs choix.

1. Les différents types de compte

Sous Windows, il existe différents types de comptes utilisateur. Chacun d'eux définit un ensemble de droits tel que l'accès aux fichiers, les modifications que vous êtes autorisées à effectuer sur le système d'exploitation, etc. D'une façon générale, suivant le type de compte choisi, l'utilisateur aura un niveau d'accès plus ou moins important sur le système d'exploitation.

Il existe trois principaux types de comptes :

- Invité ;
- Standard ;
- Administrateur.

Compte utilisateur invité

Un compte utilisateur ayant des droits de type « invité » autorise l'accès aux ressources d'un ordinateur sans authentification de ce dernier. Ce type de compte n'est que très rarement utilisé en entreprise car il présente des risques non négligeables en termes de sécurité. Par défaut ce type de compte est désactivé.

Compte utilisateur standard

Un compte utilisateur standard permet d'utiliser la plupart des fonctionnalités du système d'exploitation tant que celles-ci ne touchent pas à la sécurité de l'ordinateur ou à des paramètres communs à tous les utilisateurs.

La principale différence entre un compte utilisateur standard et un compte administrateur est le niveau d'accès de l'utilisateur aux endroits définis comme protégés par le système d'exploitation.

Compte administrateur

Un compte utilisateur ayant les droits Administrateurs (et donc faisant partie d'une façon indirecte ou non au groupe Builtin\Administrateurs de l'ordinateur) est autorisé à agir sur la totalité du système d'exploitation et ainsi de pouvoir définir des paramètres communs à tous les utilisateurs (Installation de logiciels, définition de la sécurité de l'ordinateur, etc.).

Dans la mesure où les droits de ce compte sont très étendus, il est fortement déconseillé d'utiliser celui-ci pour vos tâches courantes. Vous verrez un peu plus loin dans ce chapitre comment Microsoft a répondu au besoin de sécurisation de ces accès Administrateurs grâce à l'UAC (*User Account Control*).

Par exemple, un utilisateur standard ne peut pas, par défaut, écrire au niveau du dossier système (c:\windows) ou dans la plupart de la base de registre, tandis qu'un administrateur peut le faire. Un administrateur peut également activer/désactiver le pare-feu, configurer les politiques de sécurité, installer un service ou un pilote pour tous les utilisateurs, etc.

Dans Windows Vista/Windows 2008, les comptes utilisateur standard peuvent effectuer des tâches qui nécessitaient autrefois les privilèges administrateur comme :

- Afficher l'horloge système, le calendrier et modifier le fuseau horaire.
- Modifier les paramètres d'affichage et les polices installées.
- Modifier les options d'alimentation.
- Ajouter des imprimantes et autres périphériques.

© ENI Editions - All rigths reserved

- Ajouter et configurer des connexions VPN.
- Définir une clé WEP/WPA à un réseau sans fil.

Des tâches planifiées supplémentaires permettent désormais de définir une tâche de défragmentation ou de sauvegarde automatique. Auparavant, ces fonctionnalités ne pouvaient pas être réalisées aisément et nécessitaient la plupart du temps des privilèges administrateur.

Voici une liste non exhaustive des différents droits pour un utilisateur standard et un administrateur. Celle-ci vous permettra de vous rendre un peu mieux compte des autorisations de chacun.

Utilisateurs standard	Administrateurs
Établir une connexion réseau.	Installer/désinstaller des applications.
Établir une connexion réseau sans fil.	Installer le pilote d'un périphérique.
Modifier les paramètres d'affichages.	Installer les mises à jour Windows.
Défragmenter le disque dur (par l'intermédiaire d'un service).	Configurer le contrôle parental.
Lire un CD/DVD.	Installer un contrôle ActiveX.
Graver un CD/DVD.	Configurer le pare-feu.
Modifier le fond d'écran.	Modifier le type de compte d'un utilisateur.
Accéder à la date et l'horloge système et modifier le fuseau horaire.	Modifier les parameters UAC.
Utiliser le bureau à distance pour se connecter à des ordinateurs distant.	Configurer l'accès au bureau à distance.
Configurer les options d'alimentation de la batterie.	Créer ou supprimer un compte utilisateur.
Configurer les options d'accessibilités.	Copier ou déplacer des fichiers dans les dossiers Program Files ou Windows.
Restaurer les fichiers sauvegardés de l'utilisateur.	Définir des tâches planifiées.
Définir une synchronisation entre un périphérique mobile et l'ordinateur (Smartphone, ordinateur portable, Personal Digital Assistant (PDA)).	Restaurer la sauvegarde de fichiers systèmes.
Connecter et configure un périphérique bluetooth.	Configurer le service de mise à jour automatique.

Un quatrième type de compte était fortement utilisé sous des environnements comme Windows 2000/XP. Il s'agissait des comptes étant membre du groupe « Utilisateurs avec pouvoir ». Ce groupe était à mi-chemin entre Utilisateur Standard et Administrateurs. Il permettait en effet d'effectuer certaines tâches comme la possibilité d'écrire à certains endroits de la base de registre et du système de fichiers, sans nécessairement avoir des droits d'administrateurs. Ce type de groupe ne permettant pas de répondre à tous les besoins des applications, il a été supprimé par défaut sous Windows Vista. Il faut tout de même savoir que ce groupe reste utilisable afin de permettre une compatibilité descendante pour les applications le nécessitant. Pour cela, il faut charger un modèle de sécurité particulier (compatws.inf) dans Windows Vista afin de modifier les droits sur certains fichiers et clés de la base de registre pour permettre au groupe « Utilisateurs avec pouvoir » d'y avoir accès.

2. Le contrôle d'accès utilisateur

Le contrôle d'accès utilisateur ou User Account Control (UAC) est une des principales avancées de la nouvelle gamme

© ENI Editions - All rigths reserved

de système d'exploitation Microsoft Windows Vista et Windows Server 2008.

Cette nouvelle fonctionnalité (activée par défaut sous Windows Server 2008) permet de vous informer de toute action nécessitant des privilèges systèmes. Un jeton d'accès complet est alors créé avec les droits les plus importants de l'utilisateur puis est passé à l'application. Cela s'appelle une élévation des privilèges. L'UAC se caractérise par une élévation des privilèges automatisée, un message d'avertissement lors de cette élévation, ainsi qu'un bureau sécurisé dédié à ce message d'avertissement.

Il sera ainsi beaucoup plus compliqué à un logiciel espion de s'installer sur le système ou de venir se greffer à un processus sans que vous en soyez informé.

Il vous est désormais plus simple d'identifier les tâches qui nécessiteront des droits plus importants. L'icône en forme de bouclier accolé à certaines applications et assistants de configuration indique que ces tâches vont se lancer avec des permissions d'administrateurs de l'ordinateur.

Pour les autres applications, un message d'élévation de privilège apparaîtra si besoin.

Avant que l'élévation des privilèges ne soit effectuée, Windows Server 2008 bascule par défaut la fenêtre de confirmation demandant cette élévation de droits vers un bureau virtuel isolé et sécurisé tandis que le reste des applications continuent de s'exécuter au niveau du bureau interactif de l'utilisateur. Cela permet ainsi d'empêcher à un processus utilisateur (comme un logiciel espion) d'interagir avec la demande d'élévation de privilège et ainsi d'accepter automatiquement l'élévation.

La fenêtre de demande d'élévation pour le processus en question se trouve donc dans un environnement hermétique. Ainsi, si un attaquant choisissait de créer un exécutable permettant de reproduire avec exactitude la fenêtre d'élévation de privilège, vous n'irez pas exécuter celle-ci car son affichage ne se ferait pas dans le bureau virtuel. De même, le bureau sécurisé empêche les attaques qui consistent à truquer l'affichage du pointeur de la souris. L'attaquant peut en effet modifier l'affichage de la souris de sorte que lorsque l'utilisateur choisit de cliquer sur **Annuler**, l'action du clic de souris est effectuée sur le **Continuer** ; permettant ainsi d'exécuter l'application dangereuse. Le bureau virtuel permet ainsi de bloquer ce type d'attaque.

Par ailleurs, un mode particulier nommé **Mode d'approbation d'administrateur** est activé pour tous les membres du groupe Administrateurs (hormis le compte Administrateur intégré). Ce mode montre l'élévation de privilèges lorsqu'une application nécessitant des droits d'administrateurs est lancée.

Il est possible de configurer ces différents paramètres via une stratégie de groupe (aussi bien locale que de domaine). Pour cela, ouvrez votre éditeur de stratégie, puis rendez-vous au niveau de **Configuration ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Options de sécurité**. Les stratégies relatives à la gestion de l'UAC sont les suivantes :

Stratégies	Description
Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré	Permet de définir si le compte Administrateur intégré est soumis au Mode d'approbation administrateur ou pas. Valeur par défaut : Désactivé
Contrôle de compte d'utilisateur : passer au bureau sécurisé lors d'une demande d'élévation	Indique si la demande d'élévation doit se faire sur le bureau des utilisateurs interactifs ou sur le bureau virtuel sécurisé. Valeur par défaut : Activé
Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé	Les programmes UIAccess comme l'assistance à distance peuvent demander l'utilisation de cette option. Valeur par défaut : Désactivé
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Définit si un utilisateur connecté avec un compte administrateur obtient une invite d'élévation de privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur. Trois choix sont possibles : • **Aucune invitation** : l'élévation se produit automatiquement et en silence (Inutile de vous préciser que cette option n'est pas recommandée).

© ENI Editions - All rigths reserved

	• **Demande de consentement** : requiert une intervention de l'utilisateur pour Continuer ou Annuler l'opération d'élévation des privilèges. • **Demande d'information d'identification** : un nom d'utilisateur et mot de passe est demandé lors de la demande d'élévation des privilèges. Valeur par défaut : Demande de consentement.
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard	Définit si un utilisateur connecté avec un compte standard obtient une invite d'élévation de privilèges lors de l'exécution d'applications nécessitant des privilèges administrateur. Par défaut, un utilisateur standard aura la possibilité d'indiquer le mot de passe d'un compte administrateur. Il est également possible de désactiver cette option bien que cela n'empêchera pas l'utilisateur de faire un clic avec le bouton droit de la souris sur un exécutable et de choisir **Exécuter en tant qu'administrateur**. Valeur par défaut : Demande d'informations d'identification.
Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation	Lorsque ce paramètre est activé, l'utilisateur doit fournir son consentement lorsque Windows détecte un programme d'installation. Il n'est pas conseillé d'appliquer ce paramètre en environnement d'entreprise si l'utilisateur n'a pas les droits d'administrateur ou si un logiciel de télédistribution est déjà en place. Valeur par défaut : Activé.
Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des emplacements sécurisés	Indique que seules les applications nécessitant un niveau d'intégrité UIAccess (c'est-à-dire lors la spécification UIAccess=true dans leur manifeste d'application) doivent se trouver à un emplacement sécurisé sur le système de fichiers. Les emplacements sécurisés sont : • \Program Files\ (et sous-répertoires) • \Program Files (x86)\ (et sous-répertoires) • \Windows\System32 Valeur par défaut : Activé.
Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés	Seuls les exécutables signés et validés à l'aide d'un certificat auront l'autorisation d'élever leurs privilèges. La liste des applications d'administration peut donc être contrôlée par ce moyen. Valeur par défaut : Désactivé.
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur	Permet d'activer ou désactiver le contrôle utilisateur pour les utilisateurs qui seront Administrateurs. Valeur par défaut : Activé
Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des emplacements définis par utilisateur	Cette option assure une compatibilité avec les anciennes applications qui s'exécutaient en tant qu'administrateur et écrivaient des données d'exécution de l'application dans %Program Files%, %Windir%, %Windir%\System32 ou HKLM\Software

© ENI Editions - All rigths reserved

	Valeur par défaut : Activé

Très souvent controversé car il modifie nos (mauvaises ?) habitudes, l'UAC permet néanmoins d'assurer un niveau de sécurité bien supérieur comparé aux versions précédentes de Windows.

3. Gérer vos groupes à l'aide des groupes restreints

Les groupes restreints vous permettent de gérer les membres de groupes de sécurité afin de vous assurer du contenu de ces groupes.

Les groupes restreints sont uniquement paramétrables au niveau de stratégies de domaine. Vous ne trouverez donc pas ce paramètre au niveau d'une stratégie locale. Ce paramétrage se trouve au niveau de **Configuration Ordinateur - Paramètres Windows - Paramètres de sécurité - Groupes restreints**.

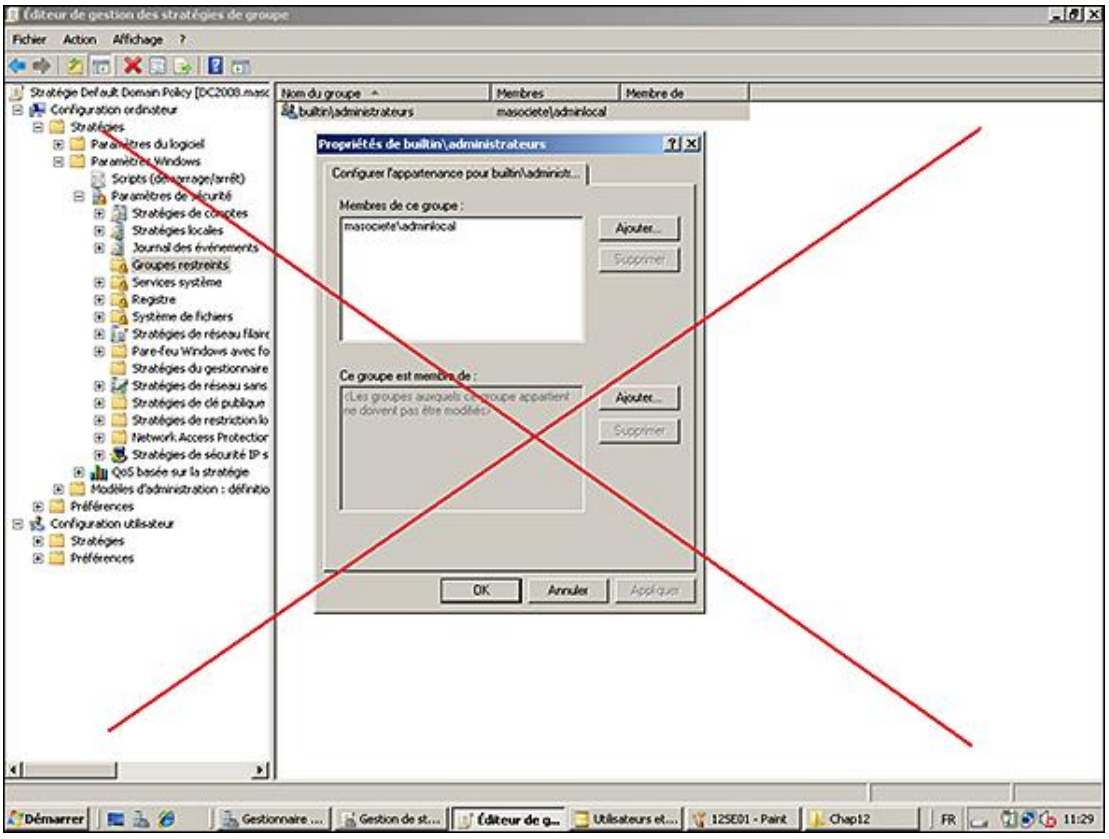
L'avantage principal, vous l'aurez compris, est de figer les membres définis au niveau de **Membre** et **Membres de...** du groupe défini comme groupe restreint. Ainsi, si par exemple l'utilisateur se voit retirer manuellement d'un groupe défini en tant que groupe restreint, il sera automatiquement ajouté à celui-ci lors de l'application de la stratégie de groupe (soit toutes les 90 minutes environ).

Avant de se lancer dans la configuration d'un groupe restreint, il convient de bien comprendre la différence entre le paramètre **Membres de ce groupe** et **Ce groupe est membre de**.

En configurant par exemple, depuis la stratégie de groupe, un groupe restreint comme le groupe local des ordinateurs nommé BUILTIN\Administrateurs (via un clic droit depuis la stratégie de groupes restreints puis **Ajouter un groupe/*Builtin\Administrators***) et en lui indiquant un groupe de domaine nommé par exemple **MaSociete\AdminLocal** au niveau de **Membres de ce groupe**, alors tous les utilisateurs du groupe **MaSociete\AdminLocal** seront Administrateurs des ordinateurs se trouvant dans le conteneur lié à la stratégie de groupe définie.

Parfait ! Me direz-vous ? Et bien pas tant que cela…

Imaginez que ce groupe restreint soit défini au niveau des ordinateurs de votre Active Directory et qu'un utilisateur ait besoin d'être membre du groupe Administrateurs de son ordinateur (il n'est pas rare que les utilisateurs d'ordinateurs portables aient ce genre de besoin). En le rajoutant au groupe **MaSociete\AdminLocal**, l'utilisateur sera en effet membre du groupe BUILTIN\Administrateurs de son ordinateur mais également administrateur de tous les autres ordinateurs !



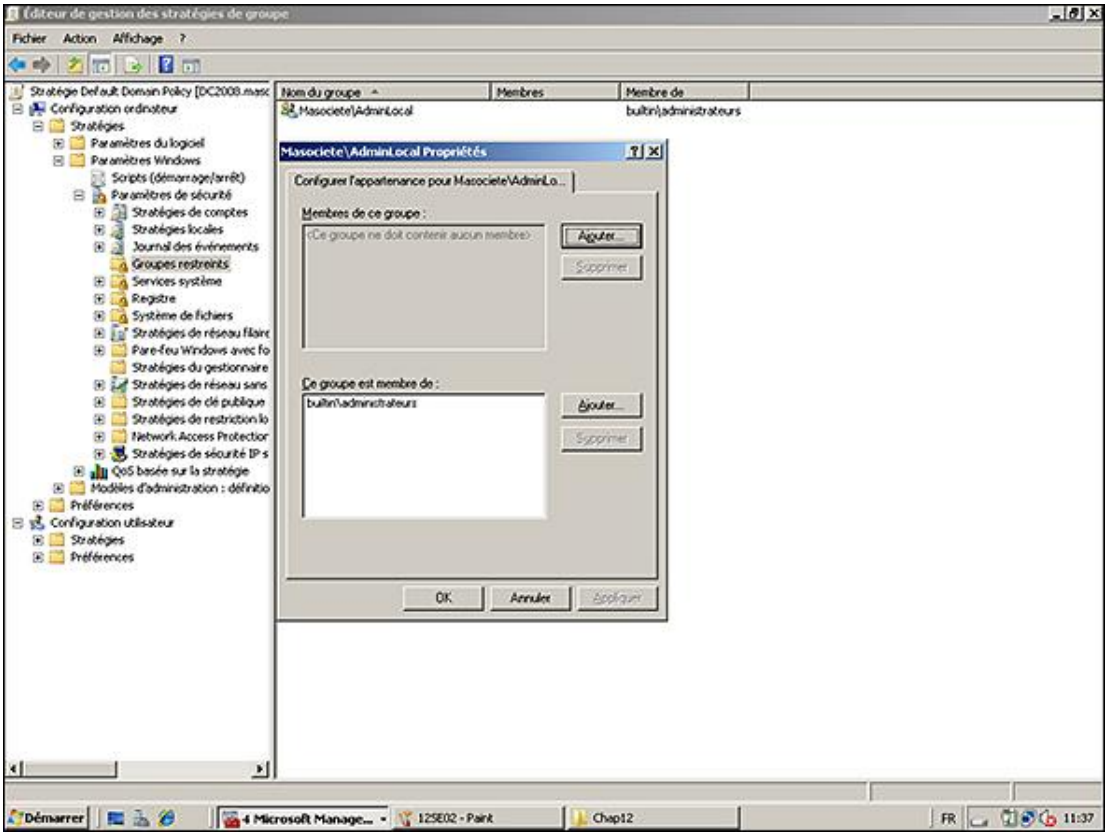
De même, si vous tentez de rajouter ce même utilisateur localement au groupe BUILTIN\Administrateurs de son ordinateur, l'application de la stratégie de groupe aura pour effet de nettoyer les membres des groupes locaux et par conséquent l'utilisateur se verra retirer les droits administrateurs.

© ENI Editions - All rigths reserved

Vous l'aurez compris, ce type de configuration n'est que peu adapté à la définition des membres des groupes au niveau des postes de travail mais il peut être très intéressant pour contrôler les membres des groupes des serveurs et contrôleurs de domaine afin de figer ces derniers.

Pour en revenir à notre utilisateur souhaitant être administrateur de son ordinateur en utilisant les groupes restreints et sans que cela n'impacte la sécurité des autres ordinateurs, il convient de définir les groupes restreints de façon un peu différente.

Il faut en effet définir un groupe restreint à partir du groupe de domaine choisi (dans notre exemple le groupe **MaSociete\AdminLocal**) et définir le paramètre **Ce groupe est membre de :** afin d'y rajouter le groupe **BUILTIN\Administrateurs** (ou BUILTIN\Administrators selon que cette stratégie de groupe est définie depuis un ordinateur français ou anglais).



Ainsi, le groupe **MaSociete\AdminLocal** a son attribut ***IsMemberOf*** figé et les utilisateurs faisant partie de ce groupe sont effectivement membres du groupe Administrateurs de tous les ordinateurs mais sans que cela n'empêche un utilisateur lambda d'être administrateur de son ordinateur.

La gestion des groupes représentant toujours un véritable défi pour nos systèmes d'information et la sécurité qui en découle, les groupes restreints répondent fortement à cette attente.

© ENI Editions - All rigths reserved

Délégation d'administration

L'un des principaux avantages d'un domaine Active Directory est de pouvoir fournir un annuaire commun à plusieurs entités au sein d'une même société. Cet annuaire partagé aide ainsi à réduire les coûts de gestion associés au maintien de l'infrastructure.

1. Approche de la délégation d'administration

Les politiques de sécurité étant généralement différentes au sein des divisions et les équipes IT n'étant pas les mêmes, il convient de trouver une solution afin de déléguer les tâches nécessaires au travail de chacun sans pour autant compromettre la sécurité de tout le domaine Active Directory.

La structure d'un domaine Active Directory est organisée par défaut de façon hiérarchique. Il est en effet possible de déléguer des tâches au niveau d'une forêt, d'un site, d'un domaine ou bien même d'une unité d'organisation. De plus, chaque objet possédant des attributs avec des DACL (*Discretionary Access Control List*) associées à ces derniers, il est également possible de déléguer des options de façon assez fine (réinitialiser le mot d'un utilisateur, autoriser la désactivation d'un compte utilisateur, etc.). Nous passerons à la pratique un peu plus loin dans ce chapitre.

Avant de vous lancer dans la configuration de la délégation de votre Active Directory, il convient de bien étudier les besoins auxquels vous devez répondre.

Une lecture (en anglais) vous permettra d'y voir un peu plus clair sur la délégation de l'administration d'un Active Directory. Elle est disponible à cette adresse http://www.microsoft.com/downloads/ details.aspx?familyid=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en

2. Délégation de comptes utilisateur

Passons maintenant à la pratique en déléguant deux actions particulièrement utiles à la hotline et au support informatique d'une entreprise. Ces services n'ayant pas pour vocation d'effectuer des tâches administratives lourdes sur l'Active Directory, il serait démesuré d'ajouter ces derniers au groupe « Administrateurs du domaine » par exemple.

Parmi les besoins les plus demandés par ces services afin de répondre aux demandes utilisateurs, vous trouverez notamment le droit de joindre un poste à un domaine Active Directory et le droit de réinitialiser les mots de passe des utilisateurs.

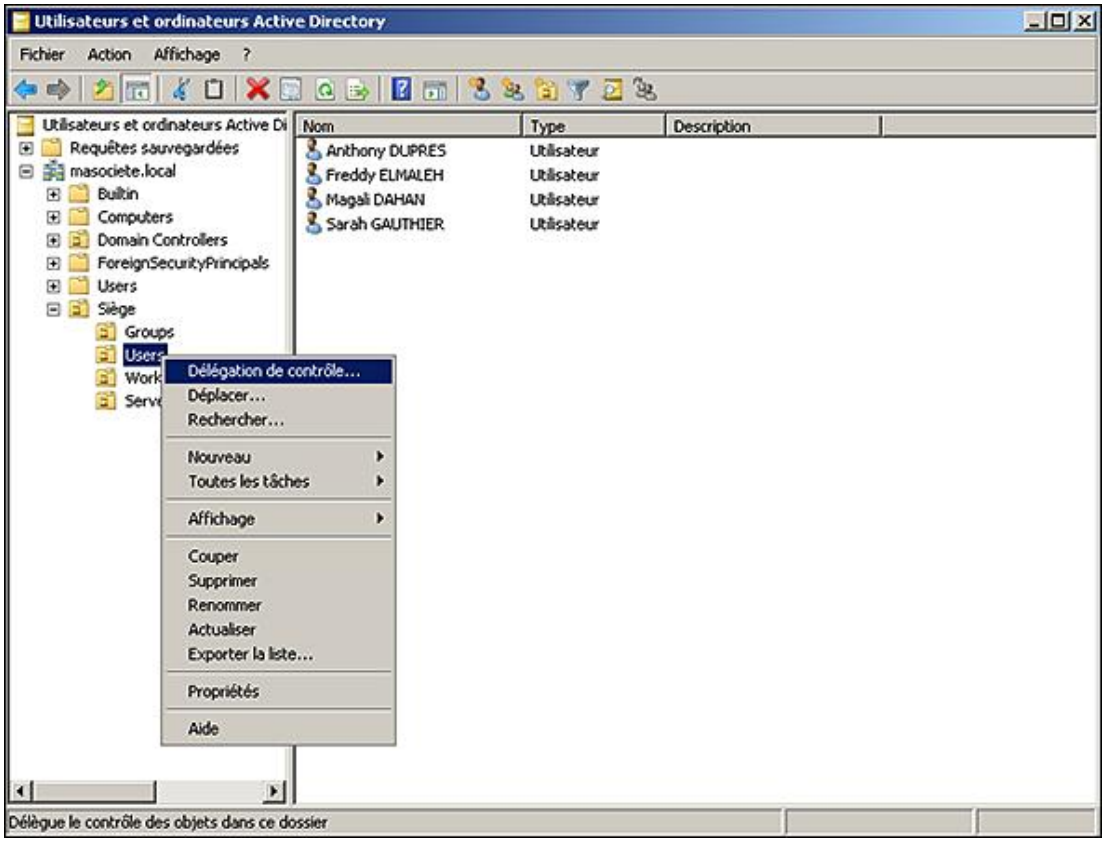
Les délégations s'effectuent généralement sur tout ou partie des objets d'une unité d'organisation (ou OU pour *Organizational Unit*) ou d'un domaine. Cela a pour but de simplifier l'administration et la gestion des droits de votre Active Directory. Inutile de vous rappeler qu'il est d'ailleurs impératif de garder une trace des délégations effectuées afin de faciliter l'administration quotidienne et les opérations de dépannage en cas de problème.

Prenons comme besoin celui du service de hotline qui souhaite pouvoir **réinitialiser les mots de passe des utilisateurs et déverrouiller leur compte**. Tous les utilisateurs de la hotline font partie du même groupe nommé **HotlineUsers**.

Afin de déléguer ces droits, Microsoft met à disposition un assistant délégation.

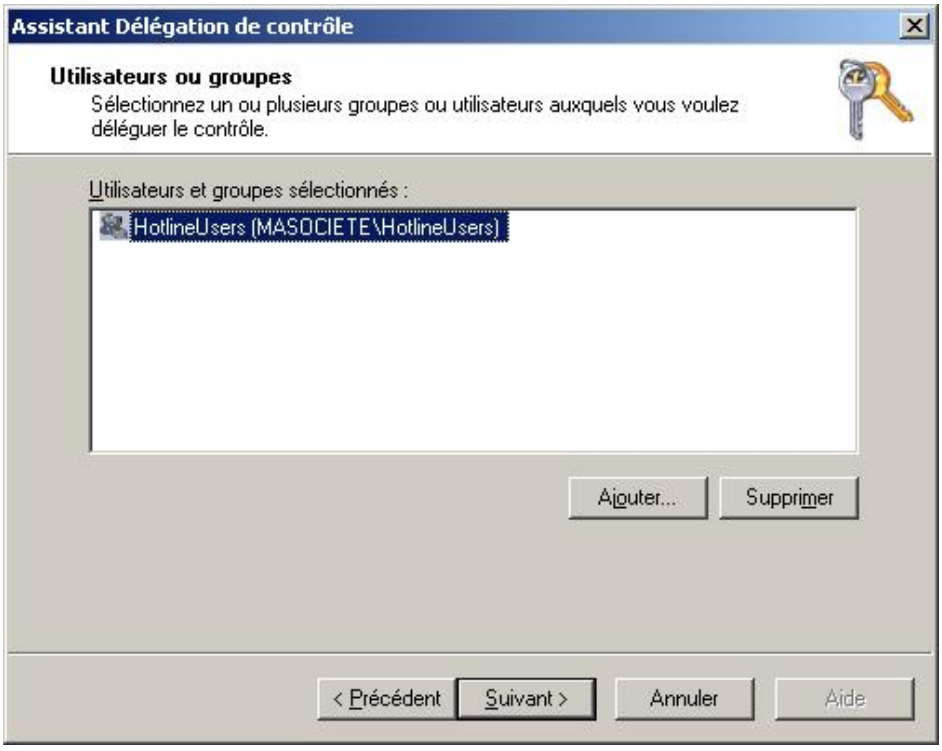
- Pour cela, placez-vous au niveau de l'objet ou du conteneur parent depuis lequel vous souhaitez effectuer une délégation de droits. Dans la plupart des cas, cette délégation s'effectue au niveau d'une unité d'organisation. Faites alors un clic avec le bouton droit de la souris sur l'objet et choisissez **Délégation de contrôle**.

© ENI Editions - All rigths reserved



- Cliquez sur **Suivant** dans l'écran de bienvenue. L'assistant vous demande alors de sélectionner les utilisateurs ou groupes pour lesquels les droits délégués seront attribués. Cliquez sur **Ajouter** puis tapez le nom de votre groupe et **Vérifier les noms** puis **OK**.

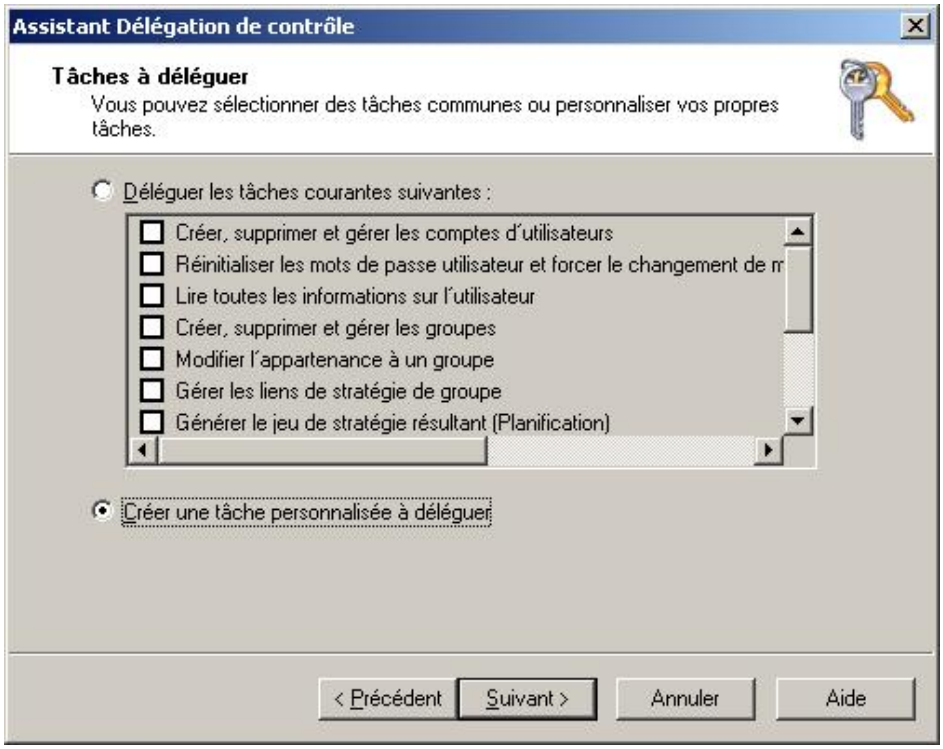
  Une fois le ou les groupe(s) ajouté(s), cliquez sur **Suivant**.



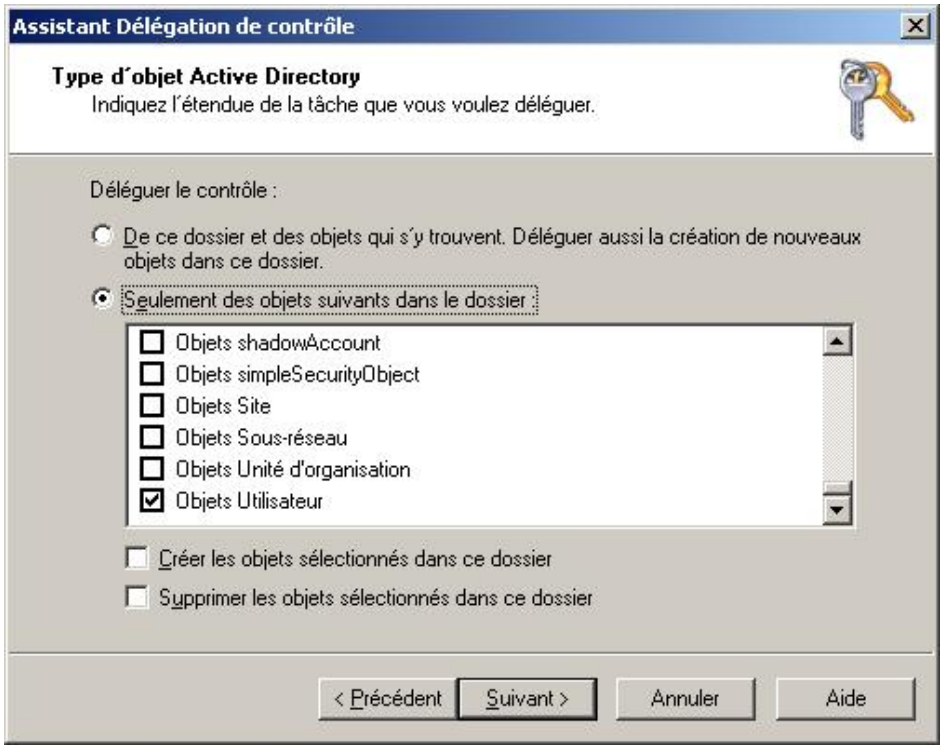
- Vous pouvez maintenant choisir le niveau de permissions qui sera appliqué à l'objet délégué. Vous avez le choix entre choisir des délégations prédéfinies pour des tâches courantes ou bien de définir une **tâche personnalisée à déléguer**.

© ENI Editions - All rigths reserved

- Dans notre exemple, nous pourrions choisir les tâches prédéfinies mais celles-ci permettraient trop de droits comparés à ce que nous souhaitons autorisés. Choisissez donc de **Créer une tâche personnalisée à déléguer** afin de pouvoir effectuer une délégation très granulaire puis cliquez sur **Suivant**.


Assistant Délégation de contrôle
Tâches à déléguer
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.
Déléguer les tâches courantes suivantes :
Créer, supprimer et gérer les comptes d'utilisateurs
Réinitialiser les mots de passe utilisateur et forcer le changement de m
Lire toutes les informations sur l'utilisateur
Créer, supprimer et gérer les groupes
Modifier l'appartenance à un groupe
Gérer les liens de stratégie de groupe
Générer le jeu de stratégie résultant (Planification)
Créer une tâche personnalisée à déléguer
< Précédent
Suivant >
Annuler
Aide

- Choisissez de déléguer le contrôle **Seulement des objets suivants dans le dossier** et cochez **Objets Utilisateur** puis **Suivant**.

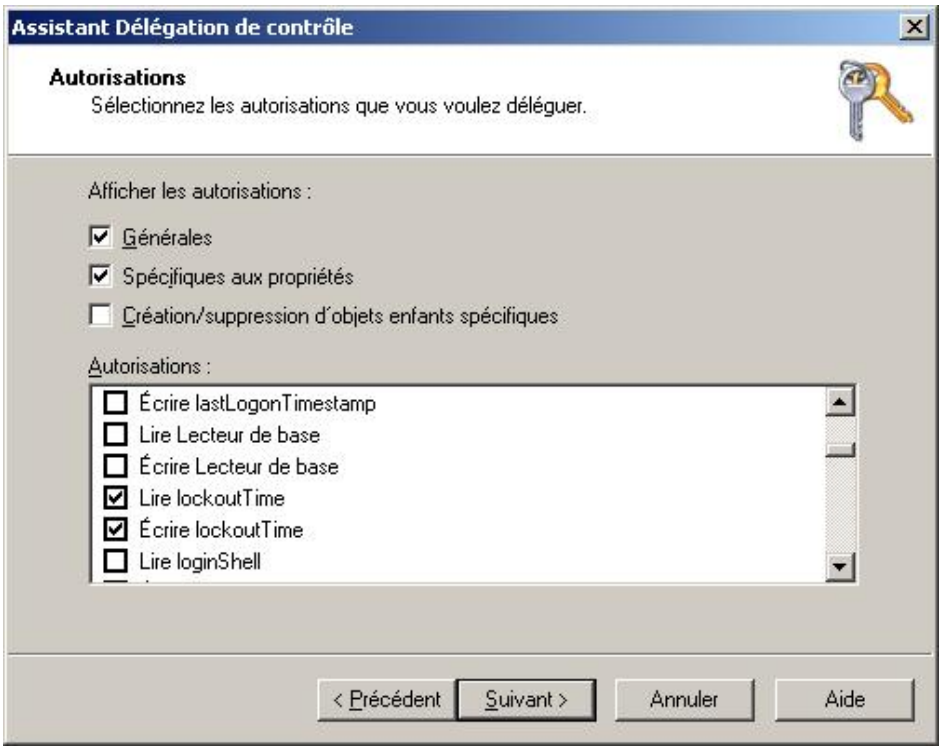

Assistant Délégation de contrôle
Type d'objet Active Directory
Indiquez l'étendue de la tâche que vous voulez déléguer.
Déléguer le contrôle :
De ce dossier et des objets qui s'y trouvent. Déléguer aussi la création de nouveaux objets dans ce dossier.
Seulement des objets suivants dans le dossier :
Objets shadowAccount
Objets simpleSecurityObject
Objets Site
Objets Sous-réseau
Objets Unité d'organisation
Objets Utilisateur
Créer les objets sélectionnés dans ce dossier
Supprimer les objets sélectionnés dans ce dossier
< Précédent
Suivant >
Annuler
Aide

- Sélectionnez alors le ou les types d'autorisations que vous souhaitez déléguer aux utilisateurs. Dans notre exemple l'attribut **Modifier le mot de passe** (ou *Change Password* en anglais) est utilisé pour la réinitialisation du mot de passe et les attributs **Lire lockout Time** (ou *Read lockout Time*) et **Ecrire lockout Time** (ou *Write lockout Time*) sont

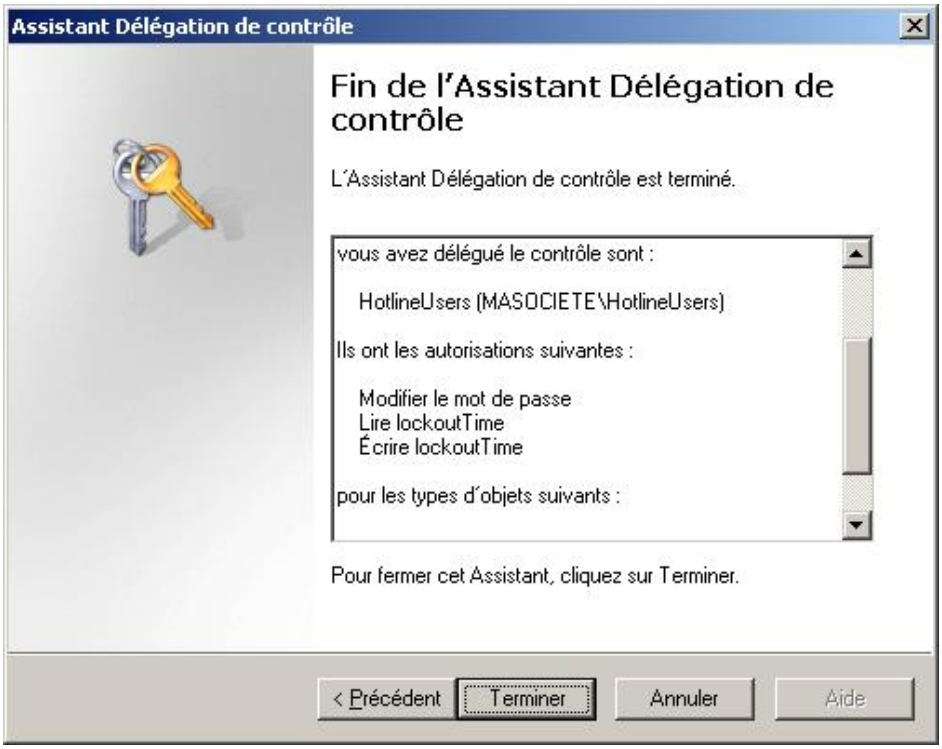
© ENI Editions - All rigths reserved

utilisés pour déverrouiller un compte utilisateur. Les deux derniers attributs ne sont visibles qu'en cochant la case **Spécifiques aux propriétés** car comme son nom l'indique, ils sont spécifiques à l'objet Utilisateur.

Une fois les trois cases cochées, cliquez sur **Suivant**.

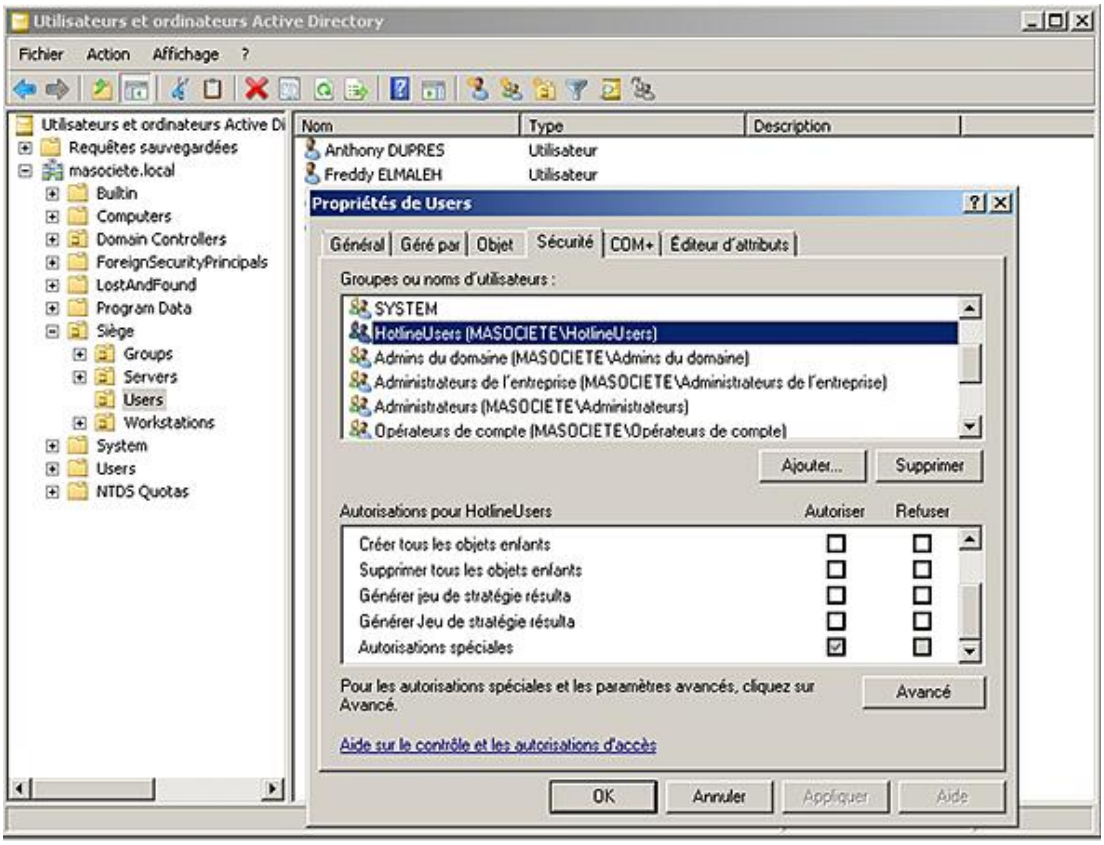


- Une fenêtre récapitulative indique les différents choix effectués au cours de l'assistant délégation. En cliquant sur **Terminer**, les ACL seront modifiés sur le conteneur choisi.



Vous pouvez lister et définir une autorisation directement depuis la console Utilisateurs et Ordinateurs Active Directory. Il faut pour cela activer les **Fonctionnalités avancées** au niveau du menu **Affichage** de la console. Ensuite, en affichant les **Propriétés** du conteneur ou de l'objet délégué, un onglet **Sécurité** sera disponible et vous permet de lister et modifier la sécurité directement depuis cet endroit.

© ENI Editions - All rigths reserved



Une fois la délégation effectuée, il est courant qu'une console MMC personnalisée soit distribuée aux personnes concernées.

L'avantage d'une console MMC personnalisée est que ces utilisateurs n'ont accès qu'à une vue limitée de l'Active Directory. Il est également possible de définir de façon exhaustive les actions disponibles (dans notre exemple, ce serait les options de **réinitialiser les mots de passe des utilisateurs** et de **déverrouiller leur compte**). Vous trouverez plus d'informations sur la façon de créer une MMC personnalisée à cette adresse http://technet.microsoft.com/en-us/library/bb742441.aspx#XSLTsection126121120120 (en anglais).

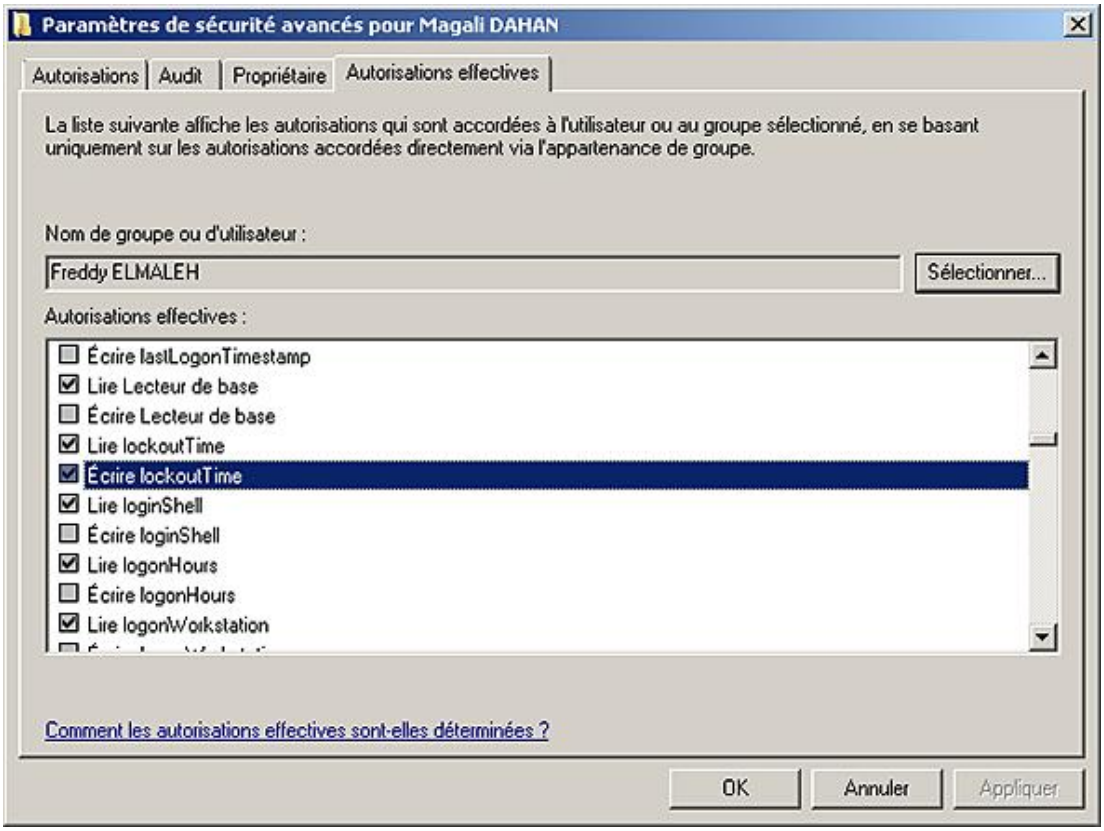
Bien qu'en ayant référencé toutes vos délégations, vous vous rendrez vite compte qu'il n'est pas toujours simple de retrouver le bon document pour savoir « qui à le droit de faire quoi ». Microsoft a pour cela inclus un onglet vous permettant de lister les **autorisations effectives** d'un compte ou groupe utilisateur sur l'objet de votre choix (options disponibles aussi bien au niveau des droits NTFS qu'au niveau de l'annuaire). Cette option peut donc être très pratique afin d'y voir plus clair dans la délégation mise en œuvre mais aussi afin de pallier des problèmes de droits souvent hérités d'objets parents difficilement identifiables. Grâce à cet outil, vous pourrez plus facilement identifier les problèmes.

- Ouvrez les **Propriétés** d'un compte utilisateur présent dans le conteneur de votre choix (par exemple, l'unité d'organisation sur laquelle vous avez défini votre délégation lors de notre précédent exercice) puis cliquez sur l'onglet **Sécurité - Avancé - Autorisations effectives** (pour rappel, si l'onglet **Sécurité** n'est pas présent, il faut choisir d'afficher les **Fonctionnalités avancées** au niveau des options d'affichage).

- Cliquez sur **Sélectionner** et indiquez le compte d'un utilisateur (dans notre exemple, il s'agit d'un compte utilisateur membre du groupe HotlineUsers).

Tous les droits que possède le compte utilisateur sur l'objet sélectionné sont alors listés. Dans l'impression écran ci-après, nous voyons bien que la permission **Écrire lockoutTime** est activée.

© ENI Editions - All rigths reserved



La délégation des tâches administratives est donc un élément important à intégrer dans vos processus d'administration afin de délimiter et limiter au mieux le rôle de chacun.

© ENI Editions - All rigths reserved

Sécurisation du réseau

La sécurisation du réseau d'entreprise est également une étape primordiale à la sécurisation générale de votre infrastructure. Cette partie a pour but de présenter les fonctionnalités intéressantes de Windows 2008 afin de venir s'implémenter au mieux dans votre infrastructure réseau existante.

1. Network Access Protection

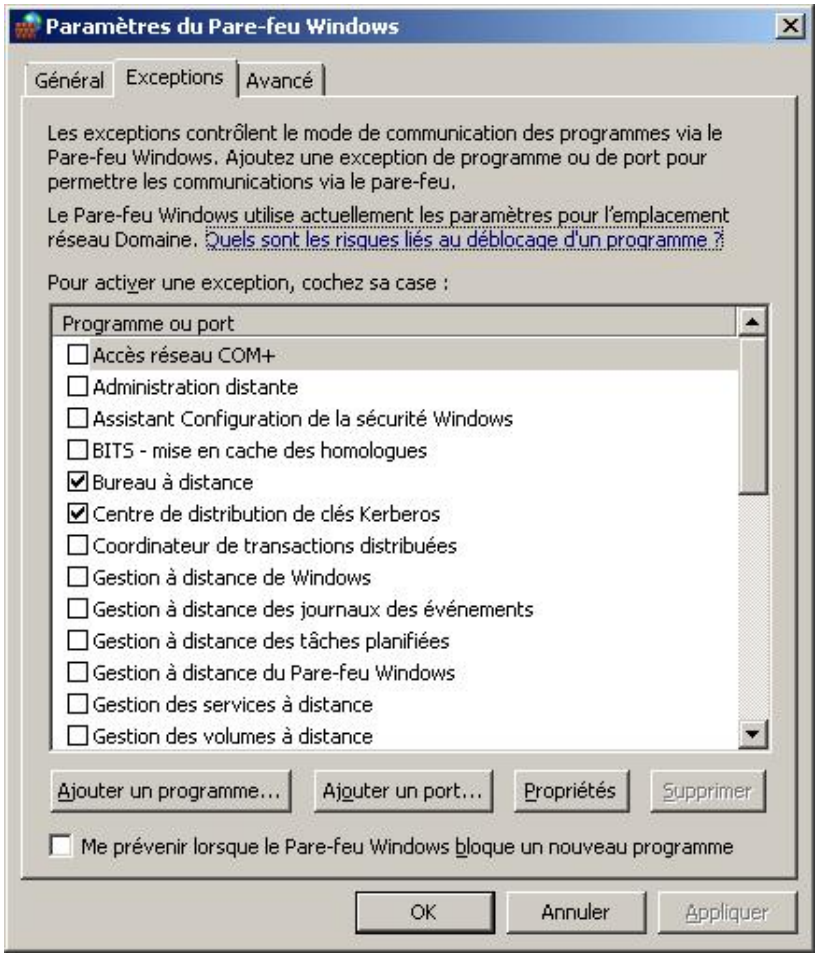
Windows Server 2008 apporte une surcouche réseau nommée NAP (pour *Network Access Protection*). Un contrôle de conformité est effectué sur tous les serveurs et postes de travail (supportant cette fonctionnalité) avant toute connexion au réseau de production.

Vous devez ainsi définir au préalable un ensemble de pré-requis de sécurité (antivirus à jour, pare-feu activé, etc). Vous serez alors capable de garantir que les ordinateurs se connectant à votre réseau d'entreprise possèdent un niveau de sécurité minimal. Si ce n'est pas le cas, ces ordinateurs sont placés en quarantaine dans un réseau dédié et non routé le temps de pouvoir répondre aux pré-requis demandés.Vous pourrez obtenir davantage d'informations sur NAP en vous référant au chapitre Mise en place des services réseaux d'entreprise.

2. Le pare-feu Windows

Windows Server 2008 met à disposition un pare-feu capable d'analyser à la fois le trafic entrant et le trafic sortant grâce à son nouveau pare-feu à sécurité avancée accessible via la console MMC du même nom.

Ce module de pare-feu n'est pas à confondre avec le pare-feu « basique » bien connu des environnements XP et accessible via la commande `firewall.cpl` puis **Modifier les paramètres**). Le pare-feu basique ne permet pas de définir des règles pour le trafic sortant mais uniquement des exceptions pour le trafic entrant.


Paramètres du Pare-feu Windows
Général
Exceptions
Avancé
Les exceptions contrôlent le mode de communication des programmes via le Pare-feu Windows. Ajoutez une exception de programme ou de port pour permettre les communications via le pare-feu.
Le Pare-feu Windows utilise actuellement les paramètres pour l'emplacement réseau Domaine. Quels sont les risques liés au déblocage d'un programme ?
Pour activer une exception, cochez sa case :
Programme ou port
Accès réseau COM+
Administration distante
Assistant Configuration de la sécurité Windows
BITS - mise en cache des homologues
Bureau à distance
Centre de distribution de clés Kerberos
Coordinateur de transactions distribuées
Gestion à distance de Windows
Gestion à distance des journaux des événements
Gestion à distance des tâches planifiées
Gestion à distance du Pare-feu Windows
Gestion des services à distance
Gestion des volumes à distance
Ajouter un programme...
Ajouter un port...
Propriétés
Supprimer
Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme
OK
Annuler
Appliquer

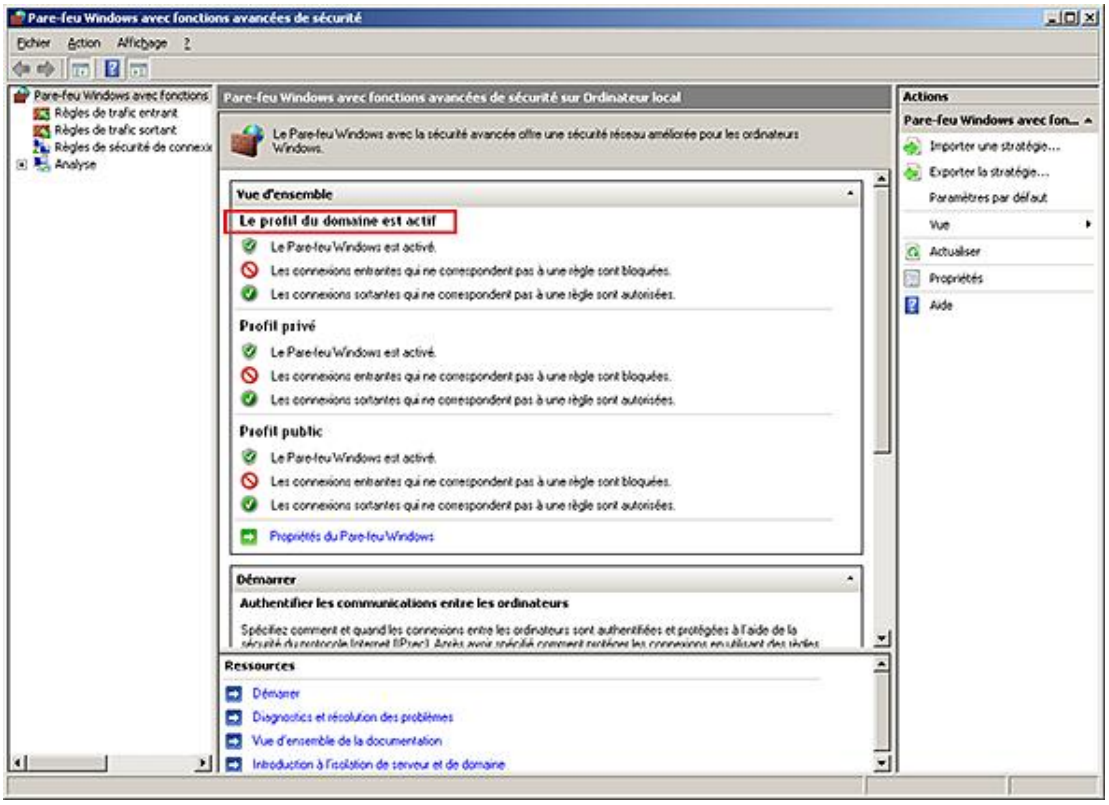
Sous Windows 2008, il est désormais possible de configurer les règles de pare-feu depuis la console MMC **Pare-feu avec fonctions avancées de sécurité** (accessible depuis les outils d'administration ou le raccourci **wf.msc**). Le pare-feu est également configurable en ligne de commande via l'argument **advfirewall** de la commande `netsh`.

© ENI Editions - All rigths reserved

La console MMC permet de définir de façon simple une configuration très précise et granulaire. Cela permet de coller au mieux avec la réalité des besoins de production.

Il est possible de définir une configuration de pare-feu différente pour chacun des trois profils de réseau existants sous Windows Server 2008. Le choix du type de profil se fait lors de la première connexion de la carte réseau et peut donc se retrouver au niveau de la console **Centre Réseau et partage**.

Vous pouvez également connaître le profil actif (et donc pour lesquelles les règles de pare-feu associées s'appliqueront) directement depuis la console MMC de configuration du pare-feu avancé.


Pare-feu Windows avec fonctions avancées de sécurité
Fichier Action Affichage ?
Pare-feu Windows avec fonctions
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de connexi
Analyse
Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local
Le Pare-feu Windows avec la sécurité avancée offre une sécurité réseau améliorée pour les ordinateurs Windows.
Vue d'ensemble
Le profil du domaine est actif
Le Pare-feu Windows est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Profil privé
Le Pare-feu Windows est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Profil public
Le Pare-feu Windows est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Propriétés du Pare-feu Windows
Démarrer
Authentifier les communications entre les ordinateurs
Ressources
Démarrer
Diagnostics et résolution des problèmes
Vue d'ensemble de la documentation
Introduction à l'isolation de serveur et de domaine
Actions
Pare-feu Windows avec fon...
Importer une stratégie...
Exporter la stratégie...
Paramètres par défaut
Vue
Actualiser
Propriétés
Aide

Pour rappel, les trois profils existants sont les suivants :

- Un **Profil de domaine** : il est automatiquement activé lorsque votre ordinateur est connecté à un domaine Active Directory.
- Un **Profil privé** : il est activé lorsque votre ordinateur est connecté à un réseau sans domaine Active Directory (aucun contrôleur de domaine disponible).
- Un **Profil public** : il est activé lorsque vous vous connectez à des réseaux que vous avez jugé peu sûrs comme les cybercafés, les aéroports, ou autres lieux dans lesquels la sécurité réseau n'est pas ou peu assurée.

Afin de centraliser le paramétrage des règles de pare-feu sur vos serveurs membres du domaine, il vous est possible (et même conseillé !) d'utiliser les stratégies de groupe. À noter, que ces stratégies de groupe sont également disponibles pour le pare-feu de Windows Vista qui est identique à celui-ci. Pour cela, saisissez **gpedit.msc** depuis le menu **Démarrer - Exécuter** puis rendez-vous dans le conteneur **Configuration Ordinateur - Modèles d'administration - Network - Network Connections - Windows Firewall**.

Vous allez maintenant configurer une règle de pare-feu afin de mieux vous rendre compte de toute l'étendue des possibilités proposées. Vous allez par exemple autoriser la connexion depuis Internet vers le port 80/TCP de votre serveur hébergeant pour l'heure un serveur Web « Apache » (nous avons délibérément choisi un serveur Web tiers afin de faciliter la compréhension des exceptions de pare-feu sur un exécutable).

- Pour cela, ouvrez la console **Pare-feu Windows avec fonctions avancées de sécuritée** (**wf.msc** depuis le Menu **Démarrer - Exécuter**), et faites un clic avec le bouton droit de la souris sur **Règles de trafic entrant** puis **Nouvelle règle**.

L'assistant se lance alors afin de choisir le type de règle de pare-feu à créer. Quatre choix s'offrent alors à vous :

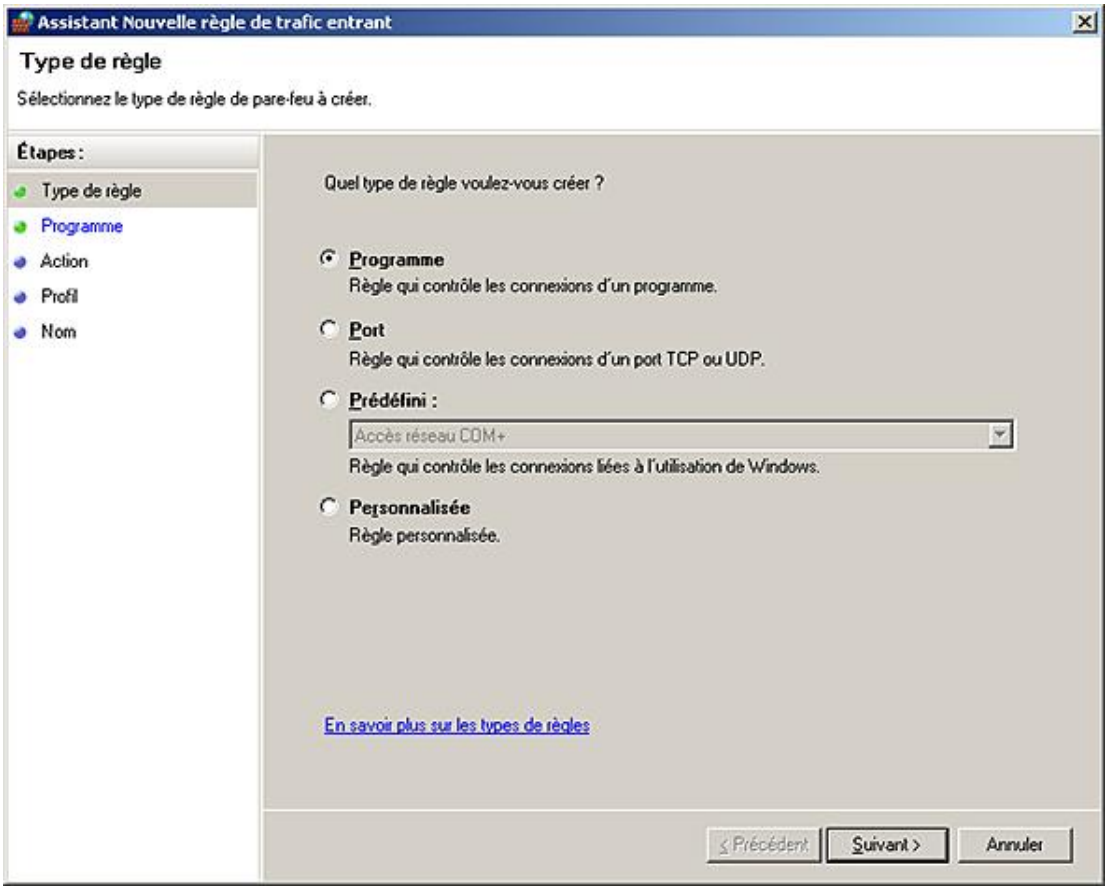
© ENI Editions - All rigths reserved

- **Programme** : cette option vous permet de définir l'exécutable pour lequel l'action définie à l'étape suivante s'appliquera.

- **Port** : permet de spécifier un port ou une liste de ports TCP ou UDP locaux de votre ordinateur.

- **Prédéfini** : règle correspondant à un service Windows (utile pour des ports ouverts dynamiquement et aléatoirement, ne nous obligeant pas à ouvrir toute une rangée de port).

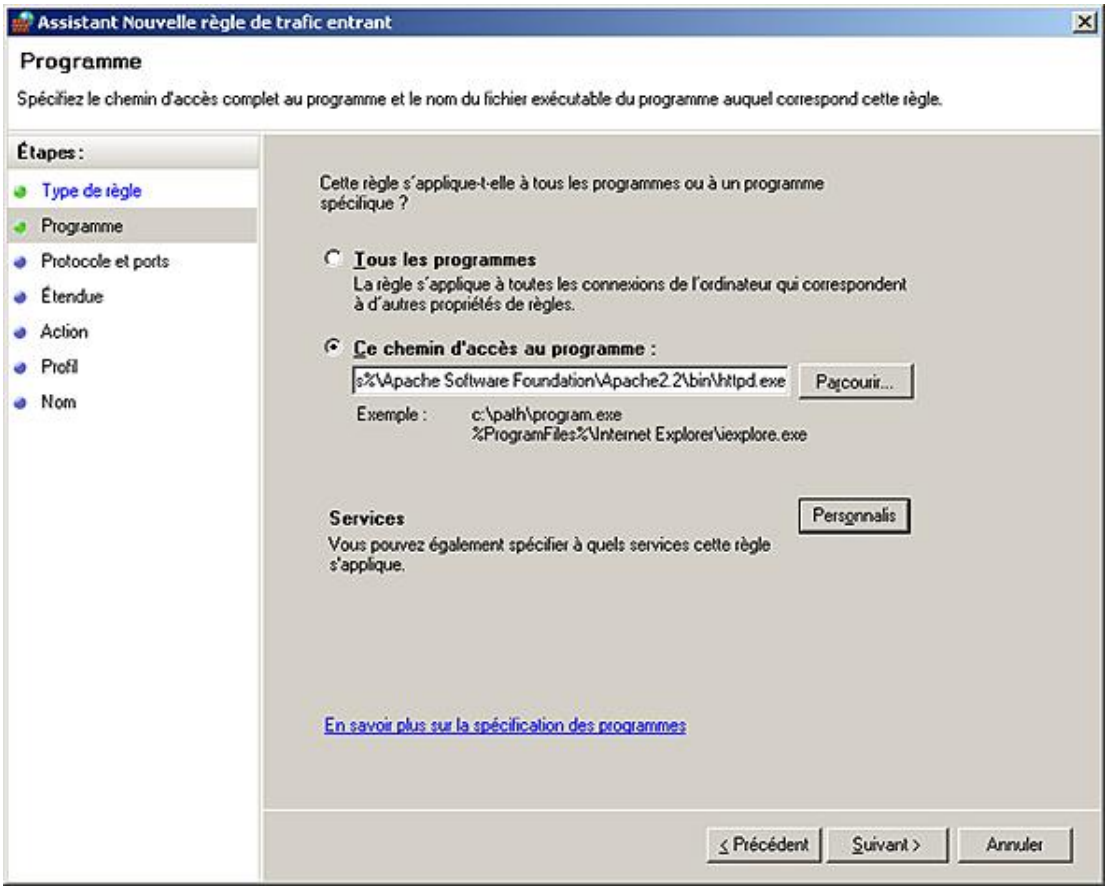
- **Personnalisée** : permet de personnaliser sa règle afin de limiter l'autorisation uniquement à un programme précis sur un port défini par exemple.



- Dans cet exemple, choisissez de créer une **règle personnalisée** puis cliquez sur **Suivant**.

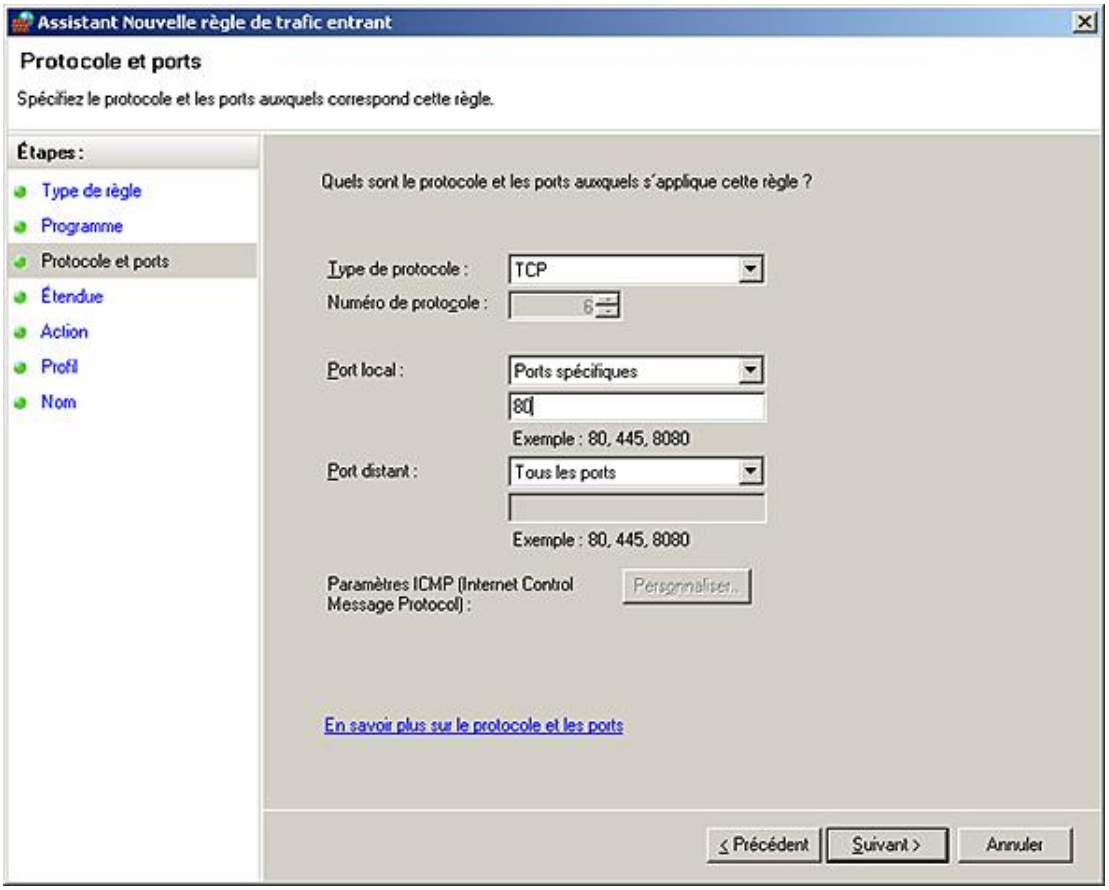
- Spécifiez alors, si vous le souhaitez, l'exécutable ou le service de votre choix puis cliquez sur **Suivant**. Dans cet exemple, indiquez le chemin complet de l'exécutable du serveur Web apache (**C:\Program Files\Apache Software Foundation\Apache2.2\bin\httpd.exe**). Il aurait également été possible de définir le service Apache via cette même étape de l'assistant.

© ENI Editions - All rigths reserved


Assistant Nouvelle règle de trafic entrant
Programme
Spécifiez le chemin d'accès complet au programme et le nom du fichier exécutable du programme auquel correspond cette règle.
Étapes :
Type de règle
Programme
Protocole et ports
Étendue
Action
Profil
Nom
Cette règle s'applique-t-elle à tous les programmes ou à un programme spécifique ?
Tous les programmes
La règle s'applique à toutes les connexions de l'ordinateur qui correspondent à d'autres propriétés de règles.
Ce chemin d'accès au programme :
s%\Apache Software Foundation\Apache2.2\bin\httpd.exe
Parcourir...
Exemple : c:\path\program.exe
%ProgramFiles%\Internet Explorer\iexplore.exe
Services
Vous pouvez également spécifier à quels services cette règle s'applique.
Personnalis
En savoir plus sur la spécification des programmes
< Précédent
Suivant >
Annuler

- Il vous reste maintenant à définir le ou les ports à autoriser (ou interdire) pour répondre à vos besoins. Le port local correspond au port de l'ordinateur sur lequel est appliqué le profil de pare-feu. Le port distant est le port situé sur l'ordinateur qui essaie de communiquer avec l'ordinateur sur lequel est appliqué le profil de pare-feu. Dans cet exemple, il vous faut autoriser le port **80/TCP** local de votre serveur pour autoriser une connexion HTTP classique.

© ENI Editions - All rigths reserved



- L'étendue de la règle peut alors être paramétrée en indiquant les adresses IP sources et de destinations pour lesquelles cette règle s'applique. Vous pouvez laisser un accès à **Toute adresse IP** dans cet exemple. Cliquez alors sur **Suivant**.

  Trois actions s'offrent à vous. Votre choix s'applique au trafic défini à l'étape précédente :

  - **Autoriser la connexion** : en d'autres termes cela permet, dans notre exemple, le trafic entrant vers le serveur Web Apache.

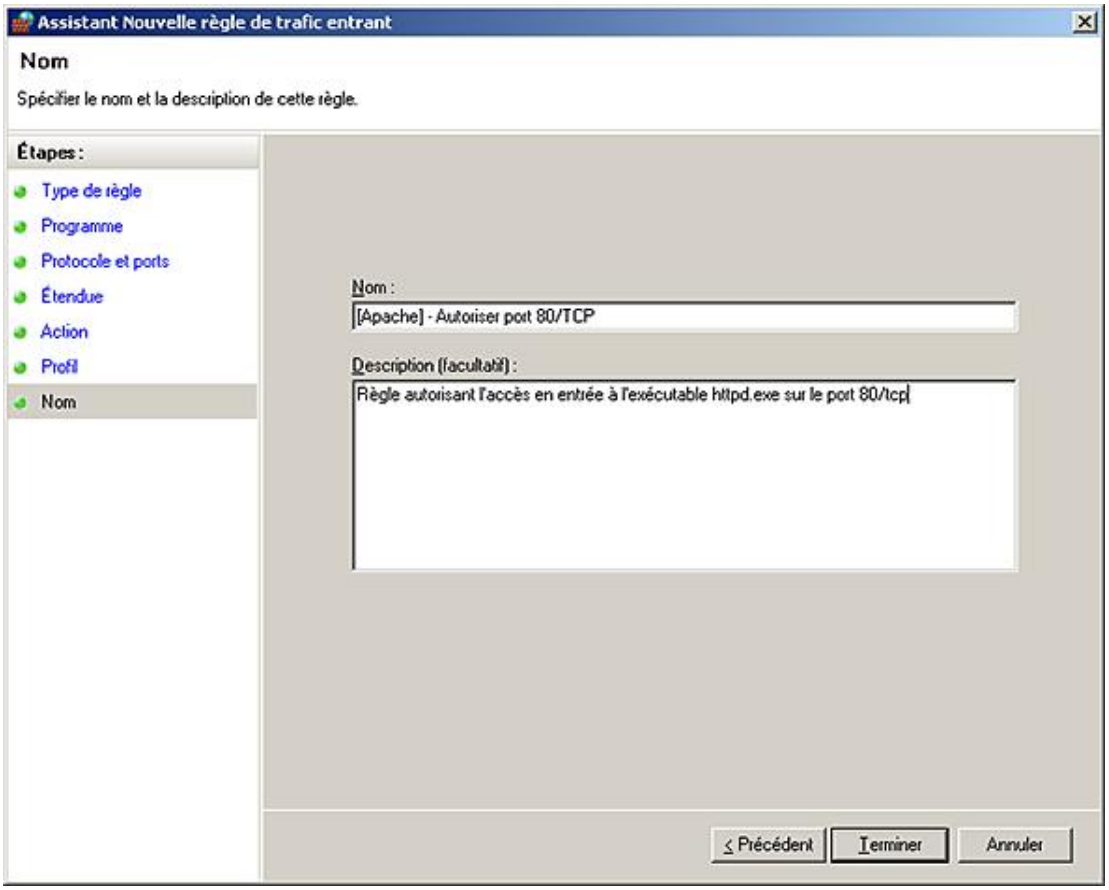
  - **Autoriser la connexion si elle est sécurisée** : permet de contrôler l'intégrité et l'authentification de chaque paquet envoyé depuis votre ordinateur en se basant sur le protocole IPSec. Nous verrons ce point un peu plus tard dans ce chapitre. L'option **Exiger le chiffrement des connexions** permet d'activer l'IPSec afin de chiffrer les paquets lors de leur transmission. Le destinataire de ces paquets doit lui aussi être configuré afin de pouvoir envoyer et recevoir ce type de trafic, sans quoi le dialogue entre les deux correspondants est impossible.

  - **Bloquer la connexion** : bloque la condition définie précédemment dans l'assistant.

  Pour notre exemple, choisissez **Permettre toutes les connexions** puis cliquez sur **Suivant**.

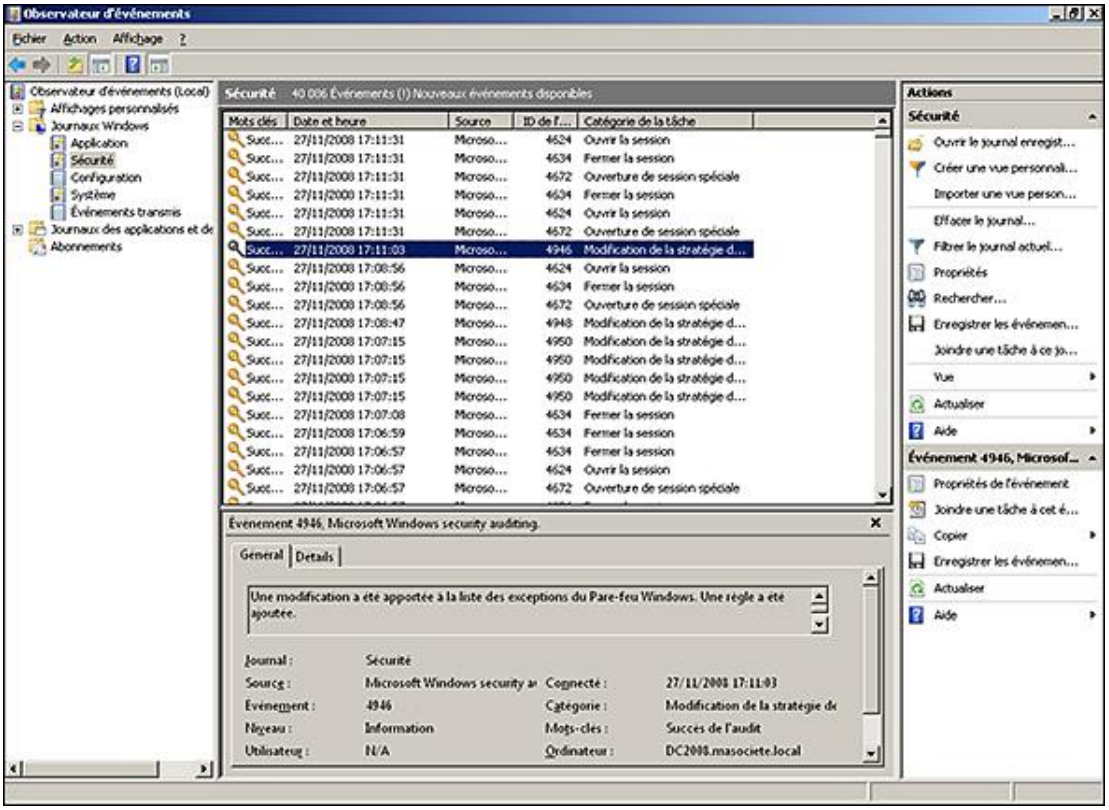
- Indiquez alors les profils de connexion pour lesquels cette règle s'appliquera puis cliquez sur **Suivant** pour donner un **Nom** à cette règle de pare-feu.

© ENI Editions - All rigths reserved



Votre règle de pare-feu est maintenant créée et effective ! Elle apparaît en haut de la liste de votre console MMC.

À noter que si l'audit des modifications des stratégies est activé (via la stratégie de groupe au niveau de **Configuration Ordinateur - Paramètres Windows - Paramètres de sécurité - Stratégies locales - Stratégie d'audit**), un évènement portant le numéro 4946 est généré dans le journal de sécurité afin d'indiquer qu'une règle de pare-feu vient d'être créée.

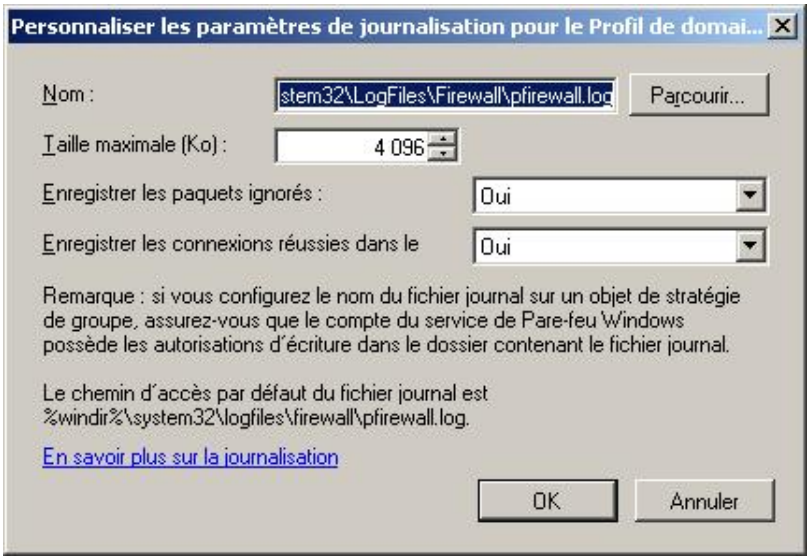

Observateur d'événements
Fichier Action Affichage ?
Observateur d'événements (Local)
Affichages personnalisés
Journaux Windows
Application
Sécurité
Configuration
Système
Événements transmis
Journaux des applications et de
Abonnements
Sécurité 40 006 Événements (!) Nouveaux événements disponibles
Mots clés Date et heure Source ID de l'... Catégorie de la tâche
Succ... 27/11/2008 17:11:31 Microso... 4624 Ouvrir la session
Succ... 27/11/2008 17:11:31 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:11:31 Microso... 4672 Ouverture de session spéciale
Succ... 27/11/2008 17:11:31 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:11:31 Microso... 4624 Ouvrir la session
Succ... 27/11/2008 17:11:31 Microso... 4672 Ouverture de session spéciale
Succ... 27/11/2008 17:11:03 Microso... 4946 Modification de la stratégie d...
Succ... 27/11/2008 17:08:56 Microso... 4624 Ouvrir la session
Succ... 27/11/2008 17:08:56 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:08:56 Microso... 4672 Ouverture de session spéciale
Succ... 27/11/2008 17:08:47 Microso... 4948 Modification de la stratégie d...
Succ... 27/11/2008 17:07:15 Microso... 4950 Modification de la stratégie d...
Succ... 27/11/2008 17:07:15 Microso... 4950 Modification de la stratégie d...
Succ... 27/11/2008 17:07:15 Microso... 4950 Modification de la stratégie d...
Succ... 27/11/2008 17:07:15 Microso... 4950 Modification de la stratégie d...
Succ... 27/11/2008 17:07:08 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:06:59 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:06:57 Microso... 4634 Fermer la session
Succ... 27/11/2008 17:06:57 Microso... 4624 Ouvrir la session
Succ... 27/11/2008 17:06:57 Microso... 4672 Ouverture de session spéciale
Événement 4946, Microsoft Windows security auditing.
General Details
Une modification a été apportée à la liste des exceptions du Pare-feu Windows. Une règle a été ajoutée.
Journal : Sécurité
Source : Microsoft Windows security a
Cognecté : 27/11/2008 17:11:03
Événement : 4946
Catégorie : Modification de la stratégie de
Niveau : Information
Mots-clés : Succès de l'audit
Utilisateur : N/A
Ordinateur : DC2008.masociete.local
Actions
Sécurité
Ouvrir le journal enregist...
Créer une vue personnali...
Importer une vue person...
Effacer le journal...
Filtrer le journal actuel...
Propriétés
Rechercher...
Enregistrer les événemen...
Joindre une tâche à ce jo...
Vue
Actualiser
Aide
Événement 4946, Microsof...
Propriétés de l'événement
Joindre une tâche à cet é...
Copier
Enregistrer les événemen...
Actualiser
Aide

Il faut également savoir qu'aucun fichier de journalisation n'est créé par défaut. Il peut être utile de configurer celui-ci

© ENI Editions - All rigths reserved

afin de faciliter la détection d'attaque sur votre serveur (scan des ports ouverts), ou le débogage permettant de trouver les ports à autoriser pour une application précise (Il suffira ainsi de tenter une connexion et de regarder dans le fichier de journalisation, les paquets qui n'ont pas été autorisés).

Afin de configurer le fichier de journalisation, faites un clic avec le bouton droit de la souris sur **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local - Propriétés**. Cliquez sur **Personnaliser** au niveau d'**Enregistrement**. Vous pouvez alors définir un chemin et un nom pour le fichier de log, une taille maximale et le type d'évènements à journaliser (paquets ignorés et/ou connexions réussies).


Personnaliser les paramètres de journalisation pour le Profil de domai...
Nom :
stem32\LogFiles\Firewall\pfirewall.log
Parcourir...
Taille maximale (Ko) :
4 096
Enregistrer les paquets ignorés :
Oui
Enregistrer les connexions réussies dans le
Oui
Remarque : si vous configurez le nom du fichier journal sur un objet de stratégie de groupe, assurez-vous que le compte du service de Pare-feu Windows possède les autorisations d'écriture dans le dossier contenant le fichier journal.
Le chemin d'accès par défaut du fichier journal est %windir%\system32\logfiles\firewall\pfirewall.log.
En savoir plus sur la journalisation
OK
Annuler

3. Le chiffrement IPSec

L'IPSec est un standard de sécurité qui fournit l'**authentification** et le **chiffrement des connexions**. Ces deux notions de sécurité ne sont pas indissociables et IPSec peut fournir l'authentification sans forcément le chiffrement et inversement. IPSec agissant sur la couche réseau du modèle OSI, il est ainsi capable de protéger n'importe quelle application réseau.

Le chiffrement des connexions via IPSec permet de rendre les attaques systèmes orientées réseau beaucoup plus difficiles. Si un attaquant venait, par exemple, à écouter (sniffer) le réseau lors d'un transfert de fichiers entre deux ordinateurs configurés pour utiliser le chiffrement IPSec, il sera dans l'impossibilité de déchiffrer les fichiers échangés !

Le second avantage du protocole IPSec est également de fournir une authentification des participants et de garantir l'intégrité des données lors d'échange réseau. IPSec peut ainsi authentifier un client réseau (via une authentification Kerberos ou un certificat par exemple) avant de permettre l'initialisation de la connexion réseau. L'attaque de type « Man in the middle » consiste à ce qu'un attaquant se fasse passer pour le serveur aux yeux du client et inversement pour le client aux yeux du serveur. Il peut ainsi écouter tout le trafic réseau entre ces deux partenaires (puis le réémettre immédiatement au vrai destinataire) et alors récupérer le mot de passe de l'utilisateur lors d'une phase d'authentification sur le domaine Active Directory par exemple.

L'authentification IPSec permet d'empêcher ce type d'attaque en authentifiant les participants et en s'assurant que les données n'ont pas été modifiées durant leur transport.

Cette authentification peut également être très utile pour définir une réplication entre des contrôleurs de domaine se trouvant sur des sites différents et ainsi garantir l'intégrité de la transaction.

Il faut également savoir que le protocole IPSec fonctionne dans deux modes possibles. Le **mode transport** ou le **mode tunnel**.

Le mode transport d'IPSec permet de protéger des communications entre deux hôtes d'un même réseau privé ou entre deux hôtes n'étant pas séparés par une translation d'adresses réseau (NAT). Dans ce dernier cas, vous pourrez mettre en œuvre de l'IPSec Nat Traversal (NAT-T) à condition que le serveur NAT et les hôtes supportent le NAT-T (cf RFC 3947).

Le mode tunnel d'IPSec protège les communications entre un hôte et un réseau ou de réseau à réseau. Ce mode est plus souple que le mode transport.

Windows Server 2008 permet donc de définir des règles d'isolation (car une authentification est nécessaire) ou de chiffrement à l'aide du protocole IPSec.

Cette configuration peut se faire de façon assez fine via l'emplacement habituel et connu des anciennes versions de Windows Server, c'est-à-dire au niveau de la stratégie de groupe **Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies de sécurité IP**. L'avantage de cette console est que vous pouvez définir le type de trafic IP que vous souhaitez autoriser. Si vos besoins se limitent cependant à définir des règles pour

© ENI Editions - All rigths reserved

des connexions "point-à-point" (sans besoin de filtrage de ports entre les deux), les **règles de sécurité de connexion** sont bien mieux adaptées car elles sont beaucoup plus faciles à mettre en œuvre.

Vous pouvez configurer vos règles de sécurité de connexion depuis la même console MMC que le pare-feu Windows avancé. Cela facilite grandement sa mise en œuvre.

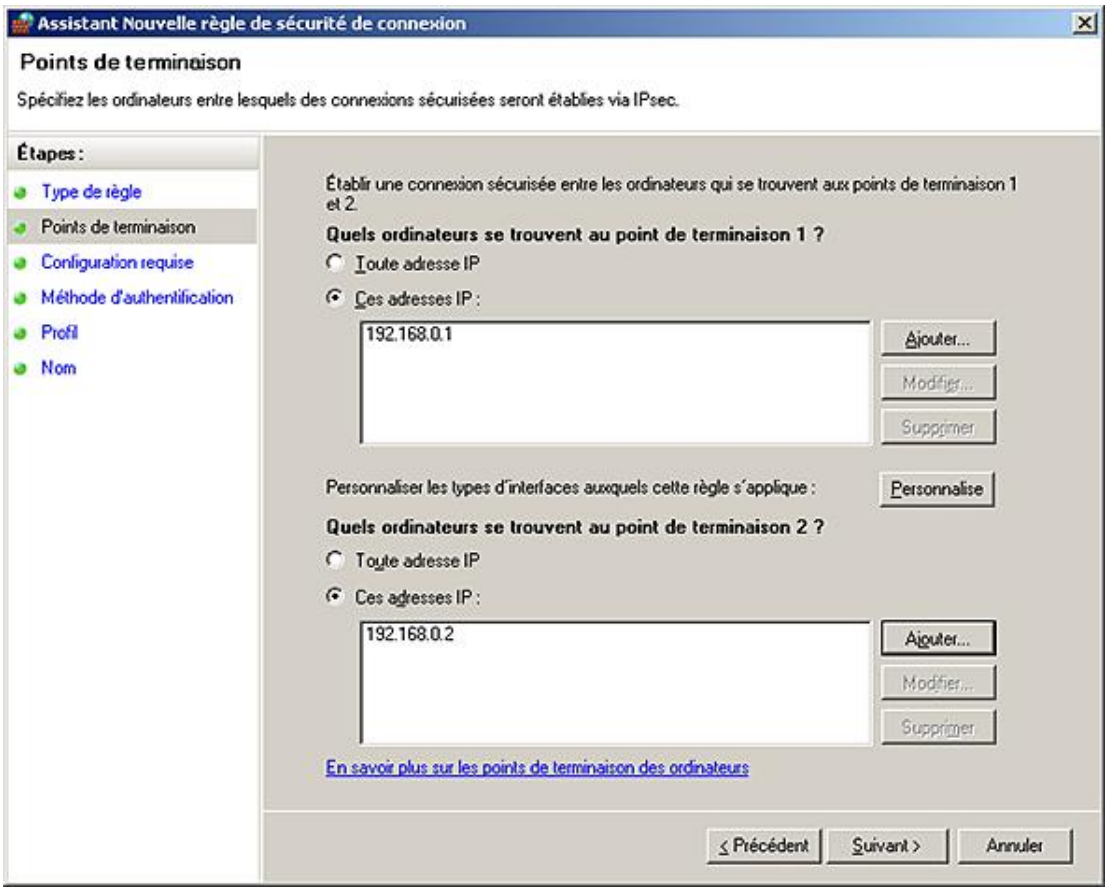
Avant de vous lancer dans la configuration de stratégies IPSec, assurez-vous d'avoir bien compris et paramétré vos stratégies IPSec sans quoi vous risquez de bloquer totalement l'accès réseau à ce serveur. Il convient donc de tester ces règles avant de les appliquer.

Vous allez maintenant tenter d'appliquer ce qui a été expliqué à l'aide d'un exemple. Dans cet exemple, vous allez chiffrer le trafic entre deux ordinateurs. Pour cela, suivez les étapes suivantes :

- Lancez la console **wf.msc** puis placez-vous au niveau de **Règles de sécurité de connexion/Action/Nouvelle règle**.

- Plusieurs types de règle de sécurité s'offrent à vous. Afin d'avoir une vision complète des possibilités, choisissez **Personnalisée** puis **Suivant**.

- Définissez alors un point de Terminaison 1 et point de Terminaison 2 correspondant à l'adresse IP de chacun des serveurs. Dans notre exemple, le point de Terminaison 1 est l'adresse IP de notre serveur local (192.168.0.1) et le point de Terminaison 2 est le serveur distant (192.168.0.2). Cliquez alors sur **Suivant**.


Assistant Nouvelle règle de sécurité de connexion
Points de terminaison
Spécifiez les ordinateurs entre lesquels des connexions sécurisées seront établies via IPsec.
Étapes :
Type de règle
Points de terminaison
Configuration requise
Méthode d'authentification
Profil
Nom
Établir une connexion sécurisée entre les ordinateurs qui se trouvent aux points de terminaison 1 et 2.
Quels ordinateurs se trouvent au point de terminaison 1 ?
Toute adresse IP
Ces adresses IP :
192.168.0.1
Ajouter...
Modifier...
Supprimer
Personnaliser les types d'interfaces auxquels cette règle s'applique :
Personnalise
Quels ordinateurs se trouvent au point de terminaison 2 ?
Toute adresse IP
Ces adresses IP :
192.168.0.2
Ajouter...
Modifier...
Supprimer
En savoir plus sur les points de terminaison des ordinateurs
< Précédent
Suivant >
Annuler

- Choisissez alors les conditions requises d'authentification. Dans notre exemple, choisissez d'**Imposer l'authentification des connexions entrantes et sortantes** puis cliquez sur **Suivant**.

  La méthode d'authentification utilisée se base sur la méthode définie au niveau des paramètres par défaut de l'IPSec. Ces paramètres sont configurables au niveau des **Propriétés** du **Pare-feu Windows avec fonctions avancées de sécurité -** onglet **Paramètres IPSec - Personnaliser**.

Tant que vous êtes à cet endroit, profitez-en pour définir l'obligation de chiffrement des données en cliquant sur **Personnaliser** au niveau de **Protection des données** (mode rapide) et en cochant la case **Demander le chiffrement de toutes les règles de sécurité de connexion pour protéger le trafic réseau**. Cliquez sur **OK** à trois reprises afin de revenir à l'assistant.

© ENI Editions - All rigths reserved

Dans cet exemple, au niveau de l'étape **Méthode d'authentification**, cliquez sur **Personnaliser** au niveau de **Avancé**. Cliquez alors sur **Ajouter** au niveau de la première authentification et choisissez **Clé pré-partagée** (ce paramètre n'est pas conseillé sur un réseau de production mais est acceptable dans le cadre de tests de mise en oeuvre).

En environnement de production, si les ordinateurs sont sur un même domaine Active Directory, l'authentification Kerberos est recommandée car elle ne nécessite pas de configuration particulière des ordinateurs concernés. Pour des ordinateurs ne faisant pas partie du même domaine, une authentification par certificat devra être utilisée. Indiquez alors la valeur **TestAuthentification** à cette clé pré-partagée. Cliquez sur **OK** à deux reprises puis **Suivant**.

- Spécifiez les profils auxquels s'applique cette règle. Les trois profils peuvent rester cochés.

- Donnez alors un nom à cette règle et cliquez sur **Terminer**.

Comme nous avons imposé l'authentification des connexions entrantes et sortantes, à partir du moment où vous cliquerez sur **Terminer**, la connexion n'est plus possible entre les deux serveurs. Il convient donc de recréer cette même règle sur le second serveur.

Comme vous avez pu le constater, Windows Server 2008 propose de nombreuses fonctionnalités de sécurité avancées. Ces dernières ne riment cependant pas nécessairement avec une perte de productivité. En effet, beaucoup de ces paramètres de sécurité sont facilement accessibles et peuvent être administrés de façon centralisée.

© ENI Editions - All rigths reserved

Introduction

Dans ce chapitre vous apprendrez à implémenter des solutions pour garantir le bien-être de votre réseau une fois celui-ci en place.

© ENI Editions - All rigths reserved

Gestion des sauvegardes

Penser qu'un système nouvellement mis en place ou qui tourne depuis longtemps ne nécessite aucune attention est illusoire. En effet, nul ne peut se prémunir d'événements inattendus pour son système d'information. Crash Serveurs, pertes de fichiers, erreur de manipulation humaine, incendie, etc. Tous ces éléments peuvent rendre instable votre système informatique et même aller jusqu'à le rendre complètement indisponible.

Plusieurs solutions proactives sont à votre disposition pour vous prémunir face à « l'incident ». L'une d'entre elles est la sauvegarde. Le choix d'une stratégie de sauvegarde adaptée aux besoins de l'entreprise est la meilleure assurance contre une perte de données.

Différents mécanismes de sauvegarde existent :

- **Complète** : cette méthode transfère sur le support de sauvegarde une copie de toutes les données concernées par la sauvegarde, indépendamment de la modification des données depuis l'exécution de la précédente sauvegarde.
- **Différentielle** : sauvegarde toutes les données qui ont été modifiées depuis la dernière sauvegarde complète.
- **Incrémentielle** : sauvegarde toutes les données qui ont été modifiées depuis la dernière sauvegarde, que ce soit une complète ou une incrémentielle.

Si dans leurs descriptifs les sauvegardes incrémentielles et différentielles sont très proches, dans les faits elles ont chacune leurs avantages et inconvénients.

Une sauvegarde différentielle nécessite moins de médias pour effectuer une restauration. En effet, seule la dernière complète ainsi que la dernière différentielle sont nécessaires.

Avantage : la restauration est rapide.

Inconvénient : le volume de données sauvegardé est plus important et les sauvegardes sont donc plus longues à être réalisées.

La sauvegarde incrémentielle prend moins de temps pour s'effectuer. Celle-ci ne sauvegarde que les éléments ayant été modifiés depuis la dernière sauvegarde (complète ou incrémentielle). Le volume à sauvegarder est donc moins important.

Avantage : les sauvegardes sont plus rapides et nécessitent moins de capacité sur les médias.

Inconvénient : la restauration est plus lente car il vous faudra utiliser plus de médias. La restauration requiert la dernière sauvegarde complète, ainsi que toutes les incrémentielles qui suivent jusqu'à la date pour laquelle vous avez besoin de restaurer.

Dans tous les cas, il faut que vous fassiez très attention à vos sauvegardes complètes. Ce sont elles qui vont déterminer le comportement des sauvegardes suivantes.

1. Windows Server Backup

Windows intègre, depuis sa version 3.1, un outil de sauvegarde appelé NTBACKUP. Avec Windows Server 2008, celui-ci a été remplacé. Le nom de son successeur est : WSB (*Windows Server Backup*).

Ne saisissez donc plus `ntbackup` dans le menu **exécuter**, autrement vous recevrez une erreur spécifiant que l'outil n'existe pas.

Windows Server Backupfournit une solution pour répondre aux besoins de sauvegarde et de restauration. Vous pouvez l'utiliser pour sauvegarder de façon complète un serveur, ou encore pour sauvegarder certains volumes, applications ou bien uniquement l'état du système.

Il peut effectuer des sauvegardes locales ou distantes en fonction de votre organisation. Les sauvegardes sont planifiables afin de s'exécuter de façon automatisées (le mécanisme reprend les tâches planifiées de Windows tout comme le faisait NTBACKUP). Il est également possible d'effectuer des sauvegardes ponctuelles.

Cette nouvelle version d'outil de sauvegarde intégrée à Windows change de façon significative les habitudes. Il apporte cependant quelques inconvénients dont :

- Impossibilité de sauvegarder un Exchange Server.
- Impossibilité de sauvegarder sur des lecteurs de bandes.

© ENI Editions - All rigths reserved

- Impossibilité d'écrire la sauvegarde sur un volume distant pour les sauvegardes planifiées.
- Le plus petit point de sauvegarde est le volume (pas de possibilité de sauvegarder uniquement un répertoire par exemple).
- Seuls les volumes locaux en NTFS peuvent être sauvegardés.

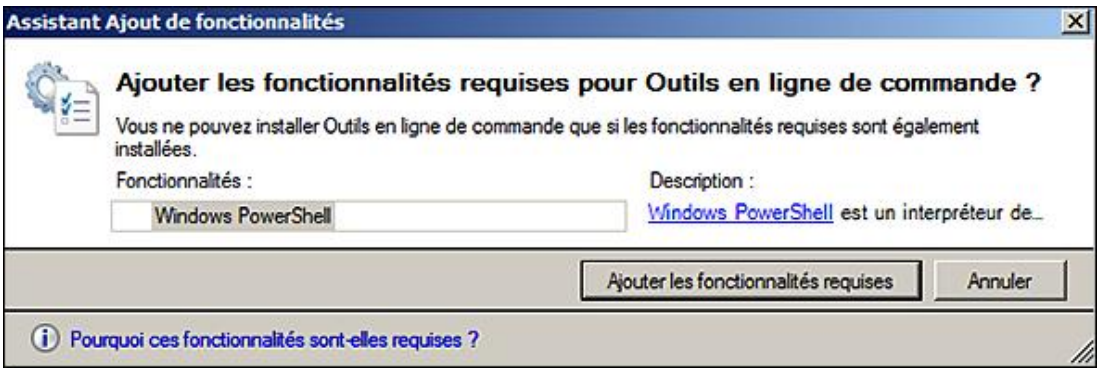
WSB ne permet pas de restaurer à partir de sauvegardes faites avec Ntbackup. Il existe cependant une version téléchargeable de l'outil compatible avec Windows server 2008 et dédiée aux restaurations. http://www.microsoft.com/downloads/details.aspx?FamilyID=7da725e2-8b69-4c65-afa3-2a53107d54a7&DisplayLang=fr

---

a. Installation de Windows Server Backup

Voici les étapes pour procéder à l'installation de Windows Backup Server :

- Allez dans la console **Gestionnaire de serveur**.
- Développez l'arborescence **Fonctionnalités** puis cliquez sur **Ajouter des fonctionnalités**.
- Cochez la case **Fonctionnalités** de la **Sauvegarde de Windows Server**.
- Cochez également la sous-case **Outils en ligne de commande**, le message suivant apparaît et vous devez cliquer sur **Ajouter les fonctionnalités requises**.


Assistant Ajout de fonctionnalités
Ajouter les fonctionnalités requises pour Outils en ligne de commande ?
Vous ne pouvez installer Outils en ligne de commande que si les fonctionnalités requises sont également installées.
Fonctionnalités :
Windows PowerShell
Description :
Windows PowerShell est un interpréteur de...
Ajouter les fonctionnalités requises
Annuler
Pourquoi ces fonctionnalités sont-elles requises ?

- Cliquez sur **Suivant**.
- À la page de confirmation, vérifiez que les fonctionnalités voulues ont bien été choisies puis cliquez sur **Installer**.

Pour installer l'outil de sauvegarde vous pouvez aussi utiliser la commande suivante : `START /W OCSETUP WindowsServerBackup`.

- À la page **Résultats de l'installation**, assurez-vous que celle-ci s'est bien déroulée puis cliquez sur **Fermer**.

Pour commencer à utiliser l'outil de sauvegarde :

- Ouvrez le menu **Démarrer** puis développez les **Outils d'administration** et enfin cliquez sur **Sauvegarde de Windows Server**.

b. Création d'une sauvegarde planifiée

Vous allez maintenant configurer votre première sauvegarde en utilisant l'assistant. Le but est ici de sauvegarder complètement la machine. Cette sauvegarde s'effectuera de manière complète tous les soirs à 23h.

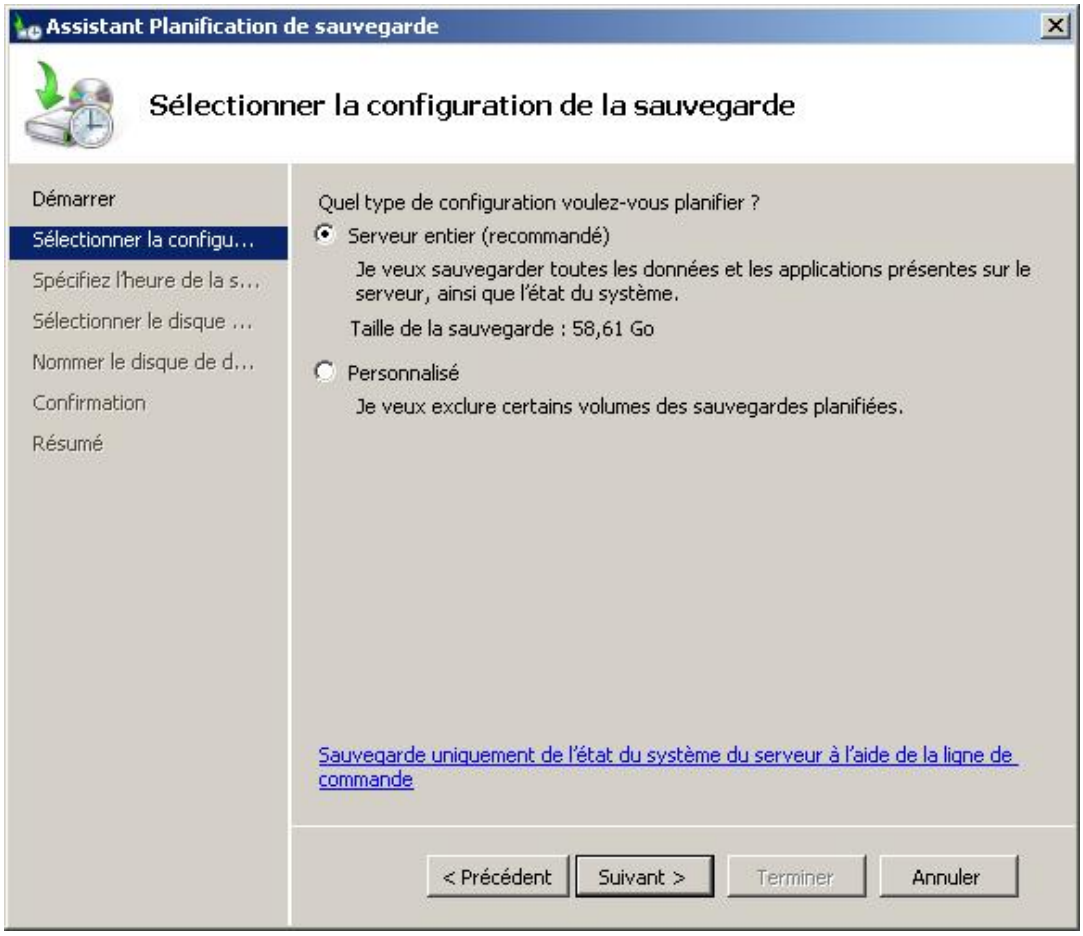
© ENI Editions - All rigths reserved

Pré-requis : posséder un second disque dur sur lequel s'effectuera la sauvegarde.

Voici les étapes à suivre :

- Dans la console **Sauvegarde de Windows Server (Local)**, dans le volet de droite cliquez sur **Planification de sauvegarde** puis cliquez sur **Suivant**.

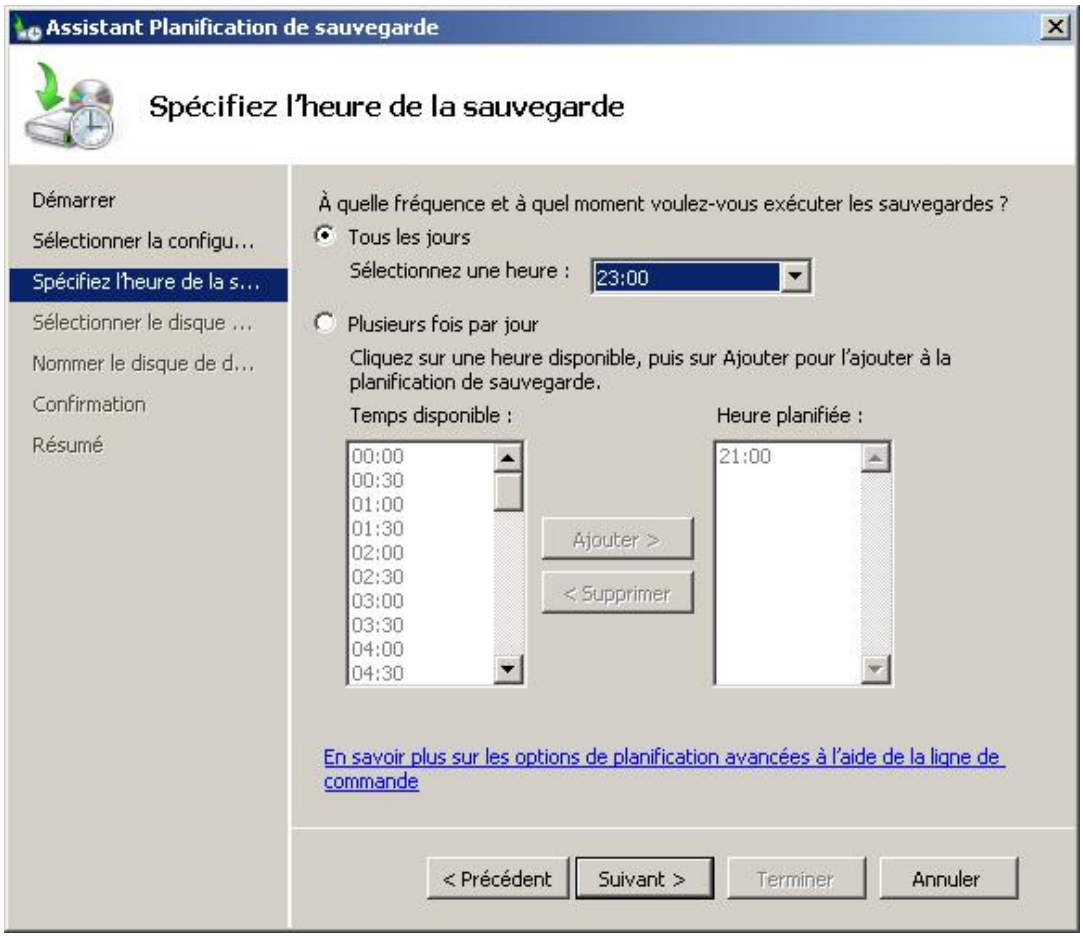
- À la page de sélection, cliquez sur le bouton radio **Serveur entier (recommandé)**.


Assistant Planification de sauvegarde
Sélectionner la configuration de la sauvegarde
Démarrer
Sélectionner la configu...
Spécifiez l'heure de la s...
Sélectionner le disque ...
Nommer le disque de d...
Confirmation
Résumé
Quel type de configuration voulez-vous planifier ?
Serveur entier (recommandé)
Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.
Taille de la sauvegarde : 58,61 Go
Personnalisé
Je veux exclure certains volumes des sauvegardes planifiées.
Sauvegarde uniquement de l'état du système du serveur à l'aide de la ligne de commande
< Précédent
Suivant >
Terminer
Annuler

- Cliquez sur **Suivant**.

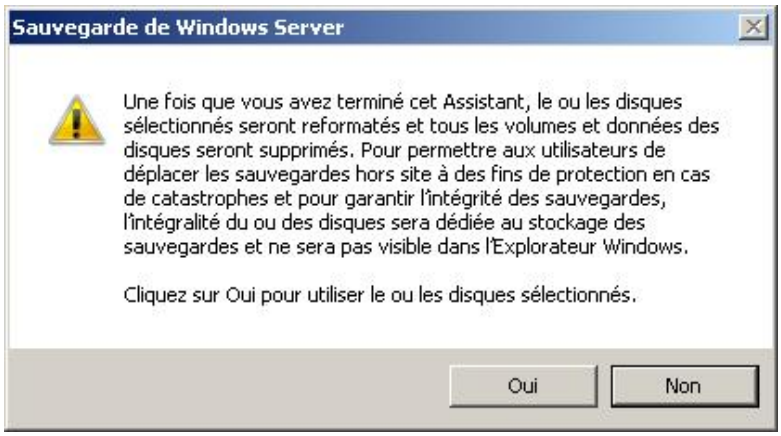
- Dans la liste déroulante, sélectionnez **23:00** puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved



- À la page de sélection du disque de destination, cliquez sur **Afficher tous les disques disponibles**.
- Sélectionnez le second disque puis cliquez sur **OK**.
- Cochez la case correspondant au disque dédié à la sauvegarde puis cliquez sur **Suivant**.

Le message suivant apparaît :


Sauvegarde de Windows Server
Une fois que vous avez terminé cet Assistant, le ou les disques sélectionnés seront reformatés et tous les volumes et données des disques seront supprimés. Pour permettre aux utilisateurs de déplacer les sauvegardes hors site à des fins de protection en cas de catastrophes et pour garantir l'intégrité des sauvegardes, l'intégralité du ou des disques sera dédiée au stockage des sauvegardes et ne sera pas visible dans l'Explorateur Windows.
Cliquez sur Oui pour utiliser le ou les disques sélectionnés.
Oui
Non

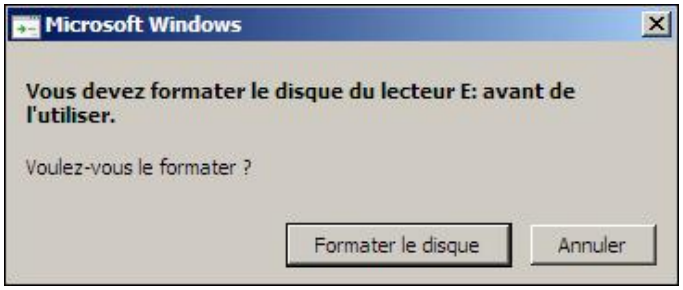
Les disques utilisés pour des sauvegardes planifiées doivent être dédiés d'où le message ci-dessus. Ils sont ensuite masqués dans l'explorateur Windows pour éviter toute erreur de manipulation.

- À la page de confirmation, cliquez sur **Terminer**.

L'assistant va formater le second disque pour le rendre utilisable pour la sauvegarde.

© ENI Editions - All rigths reserved

La fenêtre suivante s'ouvrira pour confirmer que vous voulez vraiment formater le volume :


Microsoft Windows
Vous devez formater le disque du lecteur E: avant de l'utiliser.
Voulez-vous le formater ?
Formater le disque
Annuler

- Cliquez sur **Formater le disque**.
- Une fois le formatage terminé et la planification créée, cliquez sur **Fermer**.

Votre sauvegarde est désormais opérationnelle. Vous pouvez même la retrouver dans les tâches planifiées.

Les fichiers créés par ces sauvegardes sont au format **.VHD**. De cette façon vous avez la possibilité de les intégrer directement dans des machines virtuelles à l'aide d'Hyper-V par exemple.

---

c. Outils associés à WSB et sauvegardes uniques

WSB offre également la possibilité d'effectuer des sauvegardes non planifiées. Cela peut être intéressant avant toute opération pouvant nécessiter de revenir en arrière (installation d'un nouveau produit, suppression d'un rôle, etc.). Ces sauvegardes uniques permettent également de ne pas prendre obligatoirement l'état du système dans la sauvegarde.

En suivant l'assistant **Sauvegarde unique** situé dans la console de **Sauvegarde de Windows Server**, vous pourrez :

- choisir un emplacement réseau pour effectuer la sauvegarde ;
- choisir entre une sauvegarde par Copie VSS (*Volume Shadow Copy*) ou sauvegarde complète VSS.

La copie VSS est utile si vous utilisez un autre système de sauvegarde. En effet, celle-ci laisse les attributs des fichiers intacts. De cette façon les sauvegardes qui se déroulent avec votre logiciel tiers ne sont pas affectées dans leur rotation. VSS permet également de sauvegarder des fichiers ouverts.

La sauvegarde complète VSS est utile lorsque vous n'utilisez que Windows Server Backup pour effectuer vos sauvegardes. Celle-ci, une fois son exécution terminée, met à jour l'historique de sauvegarde des fichiers.

L'outil en ligne de commande **wbadmin** est disponible avec les versions Core et Standard de Windows Server 2008. Il permet de réaliser tout ce qui est paramétrable via l'interface graphique de l'assistant de sauvegarde et plus encore.

Quelques commandes utiles avec **wbadmin.exe** :

- `wbadmin enable backup` : permet de créer et de gérer les sauvegardes planifiées.
- `wbadmin start systemstatebackup` : permet de réaliser une sauvegarde de l'état du système.
- `wbadmin start backup` : permet de lancer une sauvegarde unique.
- `wbadmin get versions` : permet de voir les détails d'une sauvegarde qui a déjà été réalisée.
- `wbadmin get items` : permet de voir quels sont les éléments contenus dans un fichier de sauvegarde.

Wbadmin a l'avantage de permettre d'implémenter les lignes dans des batch. Ces batch peuvent être eux-mêmes lancés via des tâches planifiées. Vous avez également la possibilité de lancer rapidement une sauvegarde sur un stockage réseau. Par exemple la ligne suivante permet de sauvegarder le volume E sur un partage d'une autre machine :

© ENI Editions - All rigths reserved

```
Wbadmin start backup -backuptarget:\\AUTRESERVEUR\Partage -include:E: -
User:backupadmin@masociete.local -Password:P@ssw0rd
```

Pour plus d'informations sur la syntaxe de wbadmin, rendez-vous à l'adresse http://technet.microsoft.com/en-us/library/cc754015.aspx

Bien que vous ne puissiez pas sauvegarder de ressources réseaux avec WSB, vous avez la possibilité de gérer les sauvegardes à distance.

Il vous suffit pour cela :

- Depuis la console de Sauvegarde de Windows Server, cliquez sur **Se connecter à un autre...**
- Spécifiez le nom du serveur pour lequel vous voulez gérer la sauvegarde puis cliquez sur **Terminer**.

Microsoft a significativement restreint les capacités de l'outil de sauvegarde intégré au profit de son produit System Center Data Protection Manager (DPM) 2007.Ce produit à part entière et payant offre beaucoup plus de fonctionnalités que WSB. Pour plus d'informations sur DPM : http://technet.microsoft.com/en-us/library/bb795549.aspx

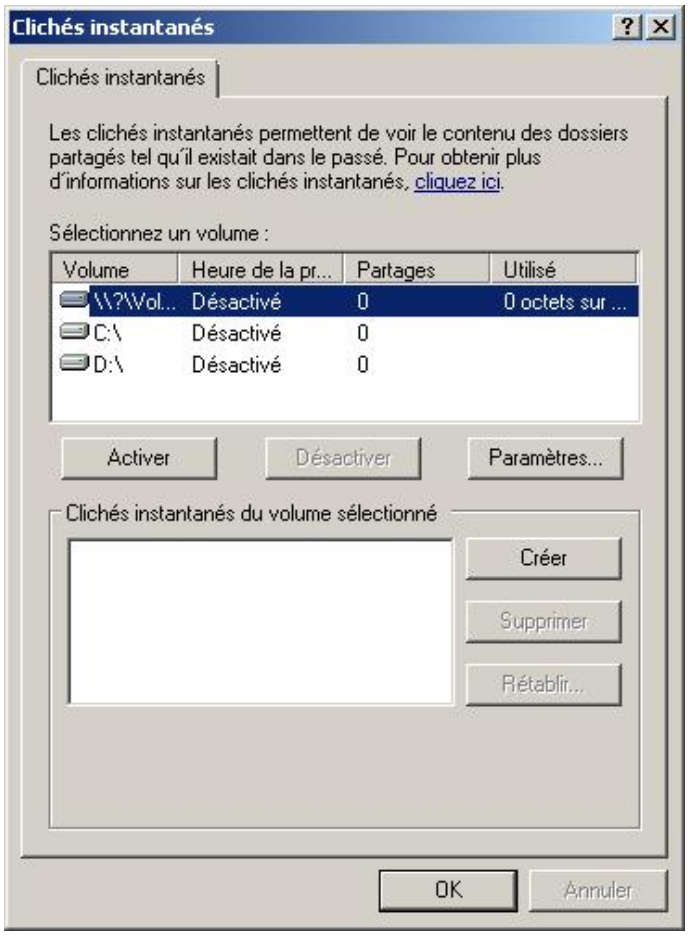
En complément des sauvegardes, vous pouvez utiliser les clichés instantanés (couramment appelés *Volume Shadow Copy*). Les clichés permettent une restauration des fichiers se trouvant sur les partages réseaux. Cette restauration s'effectue de façon très simple et très rapide.

Le principe de ce procédé est que : le serveur va initier une capture de l'état des fichiers à un moment donné puis une autre capture plus tard dans le temps. Le système va alors comparer les différences entre les états. Si un fichier a été supprimé, modifié ou autre, alors le système en gardera une copie. Plusieurs planifications peuvent être positionnées pour un même volume dans une même journée. La contrainte étant que le système ne conserve que 64 versions d'un fichier.

Les clichés instantanés s'activent au niveau des volumes. Pour les mettre en place :

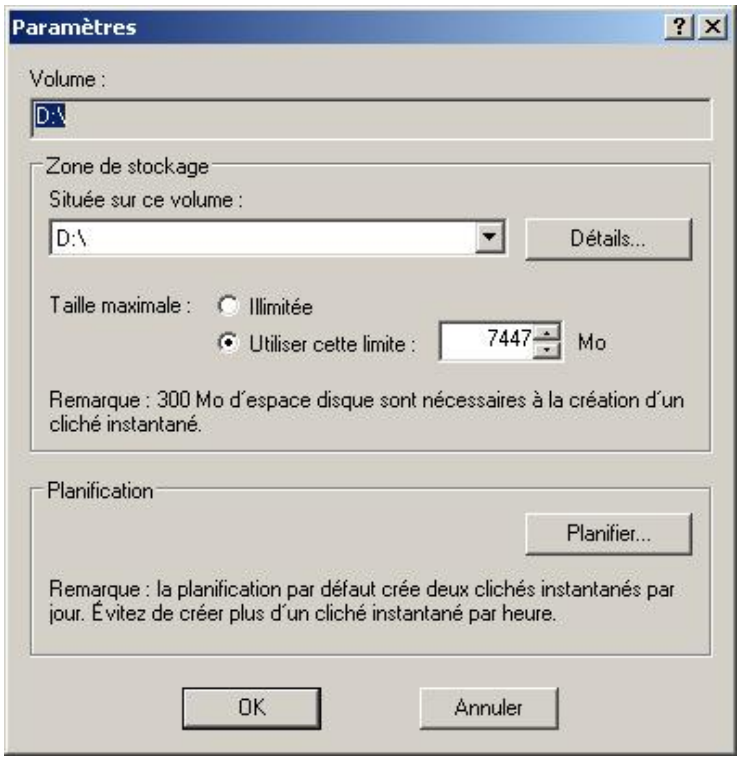
- Ouvrez votre console **Gestionnaire de Serveur**.
- Développez l'arborescence **Stockage** puis effectuez un clic avec le bouton droit de la souris sur **Gestion des disques** puis sélectionnez **Toutes les tâches / Configurer les clichés instantanés**.

© ENI Editions - All rigths reserved



Depuis cette fenêtre vous pouvez activer ou désactiver les clichés. Vous pouvez également créer un cliché manuellement en appuyant simplement sur le bouton **Créer**.

Les paramètres avancés sont gérables en cliquant sur **Paramètres** et après avoir sélectionné un volume. De là vous pouvez spécifier les planifications de ces clichés, leur emplacement de stockage ainsi que leur taille maximale.



© ENI Editions - All rigths reserved

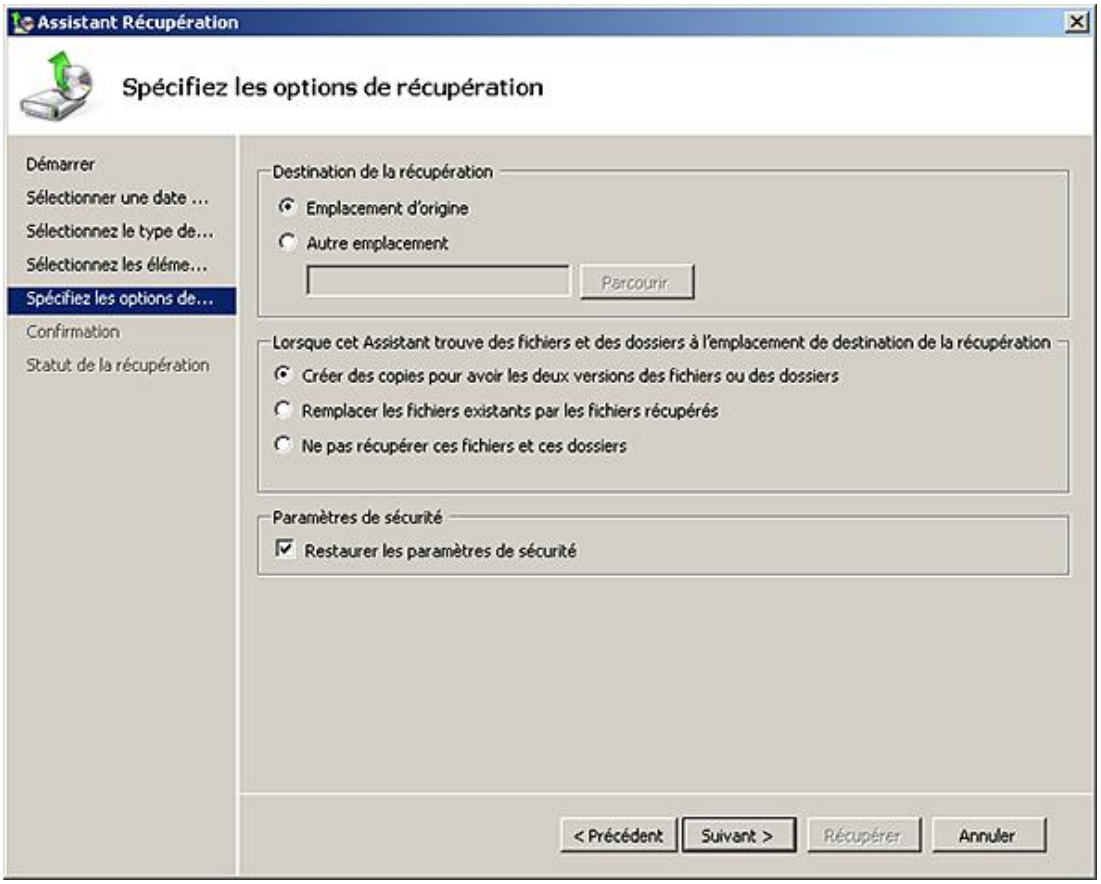
2. Restauration de données

Maintenant que vous savez comment sauvegarder vos données, vous allez voir comment les restaurer. Pour effectuer une restauration en utilisant WSB, vous devez être membre du groupe Opérateurs de sauvegarde ou du groupe Administrateurs de la machine.

a. Restauration de fichiers et/ou dossiers

Pour effectuer une restauration d'un dossier :

- Allez dans la console **Sauvegarde de Windows Server**.
- Dans le volet de droite cliquez sur **Récupérer**.
- Spécifiez le serveur pour lequel vous voulez récupérer les données puis cliquez sur **Suivant**.
- Choisissez ensuite via le calendrier, la sauvegarde que vous voulez restaurer puis cliquez sur **Suivant**.
- Choisissez le type de données que vous voulez récupérer, (**fichiers et dossiers** ou **volumes**) puis cliquez sur **Suivant**.
- Choisissez l'élément (fichier et/ou dossier) à restaurer puis cliquez sur **Suivant**.
- Spécifiez ensuite l'endroit où doit se faire la restauration, si vous voulez écraser les fichiers de destination ou bien effectuer une copie, ou ne pas récupérer les fichiers s'ils existent déjà à l'emplacement de destination. Spécifiez également si les droits NTFS doivent être récupérés.


Assistant Récupération
Spécifiez les options de récupération
Démarrer
Sélectionner une date ...
Sélectionnez le type de...
Sélectionnez les éléme...
Spécifiez les options de...
Confirmation
Statut de la récupération
Destination de la récupération
Emplacement d'origine
Autre emplacement
Parcourir
Lorsque cet Assistant trouve des fichiers et des dossiers à l'emplacement de destination de la récupération
Créer des copies pour avoir les deux versions des fichiers ou des dossiers
Remplacer les fichiers existants par les fichiers récupérés
Ne pas récupérer ces fichiers et ces dossiers
Paramètres de sécurité
Restaurer les paramètres de sécurité
< Précédent
Suivant >
Récupérer
Annuler

- À la page de confirmation, vérifiez les éléments choisis puis cliquez sur **Récupérer**.

b. Restauration de l'état du Système

© ENI Editions - All rigths reserved

En cas de défaillance majeure du système, vous devrez restaurer celui-ci. Cette opération s'apparente à une restauration complète, mais la différence est que vous ne restaurez pas les volumes contenant les données. Seuls les volumes critiques sont récupérés.

Cette opération peut s'effectuer sur la même machine ou, dans le cas d'un remplacement de matériel sur une machine différente. Attention, la machine de remplacement doit cependant posséder des caractéristiques matérielles similaires.

La restauration du système est la manière la plus pratique de réparer des rôles de serveurs corrompus ou encore de restaurer Active Directory. Attention, il n'est pas possible d'effectuer une restauration partielle de l'état du système.

La restauration de l'état du système sur un contrôleur de domaine effectue une restauration non autoritaire de l'Active Directory.

Voici les étapes à suivre pour procéder à la restauration de votre système :

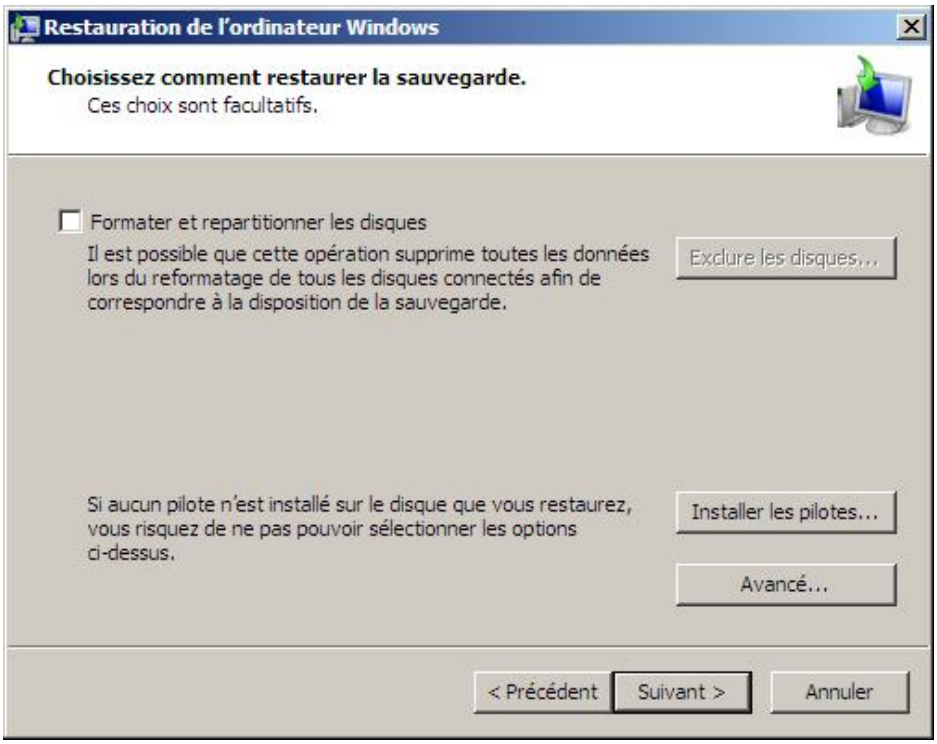
- Démarrez votre serveur à partir du CD d'installation de Windows Server 2008.
- Choisissez les paramètres de langues voulus puis cliquez sur **Suivant**.
- Cliquez sur **Réparer l'ordinateur**.
- Dans la fenêtre **Options de récupération système**, sélectionnez votre OS s'il est présent, cliquez directement sur **Suivant** s'il s'agit d'un nouveau matériel.
- Dans la fenêtre qui apparaît, cliquez sur **Restauration de l'ordinateur Windows**.

Options de récupération système
Choisir un outil de récupération
Système d'exploitation : Microsoft Windows Server 2008 sur (C:) Disque local
Restauration de l'ordinateur Windows
Restaurer tout votre serveur ou votre ordinateur personnel à partir d'une image de sauvega
Outil Diagnostics de la mémoire Windows
Vérifier les erreurs matérielles de mémoire de l'ordinateur
Invite de commandes
Ouvrir une fenêtre d'invite de commandes
Arrêter
Redémarrer

Notez qu'un outil de diagnostic de la mémoire a été directement intégré aux outils de réparation de Windows Server 2008.

- Choisissez la sauvegarde à restaurer. Puis cliquez sur **Suivant**.
- Choisissez ensuite les options facultatives (formatage et repartitionnement des disques, installation de pilotes, etc.) puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Restauration de l'ordinateur Windows
Choisissez comment restaurer la sauvegarde.
Ces choix sont facultatifs.
Formater et repartitionner les disques
Il est possible que cette opération supprime toutes les données lors du reformatage de tous les disques connectés afin de correspondre à la disposition de la sauvegarde.
Exclure les disques...
Si aucun pilote n'est installé sur le disque que vous restaurez, vous risquez de ne pas pouvoir sélectionner les options ci-dessus.
Installer les pilotes...
Avancé...
< Précédent
Suivant >
Annuler

- Cliquez sur **Terminer** puis cochez la case de confirmation et enfin cliquez sur **OK**.
- Attendez que le système redémarre automatiquement pour que la restauration soit complètement terminée.

3. Grappe RAID

Une méthode alternative de fiabilisation des données existe. Très répandue dans les environnements serveurs et en expansion auprès des particuliers, cette technologie s'appelle RAID (*Redundant Array of Independants Disks*).

D'un point de vue simplifié, cette technologie permet de stocker les informations sur des disques durs multiples afin d'améliorer, en fonction du type de RAID choisi, la tolérance de pannes et/ou les performances de l'ensemble.

Seuls les trois niveaux de RAID standard seront décrits dans ce chapitre à savoir : les RAID 0, RAID1 et RAID5. En fonction du niveau de RAID choisi, vous obtenez :

- soit un système de répartition qui améliore ses performances (RAID0) ;
- soit un système de redondance qui donne au stockage des données une certaine tolérance aux pannes matérielles (RAID1) ;
- soit les deux à la fois (RAID5).

Le système RAID est donc capable de gérer la répartition et la cohérence de ces données. Ce système de contrôle peut-être purement logiciel, ou utiliser un matériel dédié.

En RAID logiciel, le contrôle du RAID est intégralement assuré par une couche logicielle du système d'exploitation. Cette couche s'intercale entre la couche d'abstraction matérielle (pilote) et la couche du système de fichiers.

Dans le cas du RAID matériel, une carte ou un composant est dédié à la gestion des opérations. Du point de vue du système d'exploitation, le contrôleur RAID matériel offre une virtualisation complète du système de stockage. Le système d'exploitation considère chaque volume RAID comme un disque et n'a pas connaissance de ses constituants physiques.

Caractéristiques des niveaux de RAID :

- Le RAID0 ou agrégat par bandes est le plus performant ; il est par contre le moins fiable. Il offre un cumul des disques. Par exemple trois disques de 500 Go en RAID0 vous fournissent un volume de 1,5To. Inconvénient majeur de cette technologie, si un des disques vient à tomber en panne, les données situées sur les autres sont également perdues.

© ENI Editions - All rigths reserved

- LE RAID1 ou miroir fournit de bonnes performances en écriture tout en assurant une tolérance de pannes. Dans le cas de deux disques en RAID1, les informations sont écrites de façon identique sur les deux disques. Deux disques de 500 Go en RAID1 fournissent un espace de stockage de 500 Go. Le second disque servant de « réplica » au premier. Les performances globales restent néanmoins inférieures à un RAID0.

- Le RAID5 ou agrégat par bandes avec parité est le plus performant en termes de lecture. Les informations sont réparties sur les différents disques de sorte à ne pas perdre de données en cas de panne d'un des disques. Ce niveau de RAID requiert un minimum de trois disques. Trois disques de 500 Go configurés en RAID5 offrent un espace de stockage de 1 To.

Sous Windows Server 2008, les opérations de configuration des volumes en RAID se font depuis votre console **Gestionnaire de Serveur**. Ensuite il faut aller dans l'arborescence de stockage. Les options proposées vous permettront d'ajouter facilement un volume miroir ou de créer un agrégat.

Pour pouvoir configurer des volumes en RAID sous Windows Server 2008, il faut avoir converti les disques en dynamique au préalable.

Windows Server 2008 comme ses prédécesseurs ne permet pas de configurer le volume système en RAID5.

© ENI Editions - All rigths reserved

Gestion des mises à jour

1. Présentation de WSUS

Un autre moyen de vous prémunir contre d'éventuels problèmes est de vous assurer que vos machines clientes et serveurs sont bien mises à jour. Sur de petits parcs, configurer sur chaque poste les mises à jour en automatique est bien souvent suffisant. Sur de grands parcs informatiques, dans lesquels les configurations machines sont strictes, il est parfois nécessaire de tester un patch avant de le déployer de façon centralisée sur tous les postes.

Microsoft met gratuitement à disposition l'outil WSUS (*Windows Server Update Services*) en version 3.0 avec SP1. Cet outil permet le déploiement des dernières mises à jour pour les produits Microsoft. En l'utilisant vous pouvez gérer intégralement la distribution des mises à jour (heure de déploiement, quels sont les patchs à déployer, etc.)

Vous avez grâce à WSUS, un outil de centralisation et de suivi de la gestion des mises à jour. Il vous est possible en un seul coup d'œil de voir quel poste n'a pas reçu les dernières mises à jour nécessaires et de les lui pousser.

Suivant votre infrastructure, WSUS peut se mettre à jour avec le site Microsoft Update ou encore avec un autre serveur WSUS. Les clients compatibles avec WSUS commencent à partir de Windows 2000 SP4. Outre les systèmes d'exploitation, WSUS permet la mise à jour des applicatifs Microsoft les plus courants (SQL Server, Exchange Server, Office, etc.).

2. Installation de WSUS

WSUS 3.0 avec SP1 est disponible en téléchargement à l'adresse suivante :

http://www.microsoft.com/downloads/details.aspx?FamilyId=F87B4C5E-4161-48AF-9FF8-A96993C688DF&displaylang=en#Requirements

Pré-requis : vous devez avoir installé le rôle de **Serveur Web (IIS)** avec les fonctionnalités :

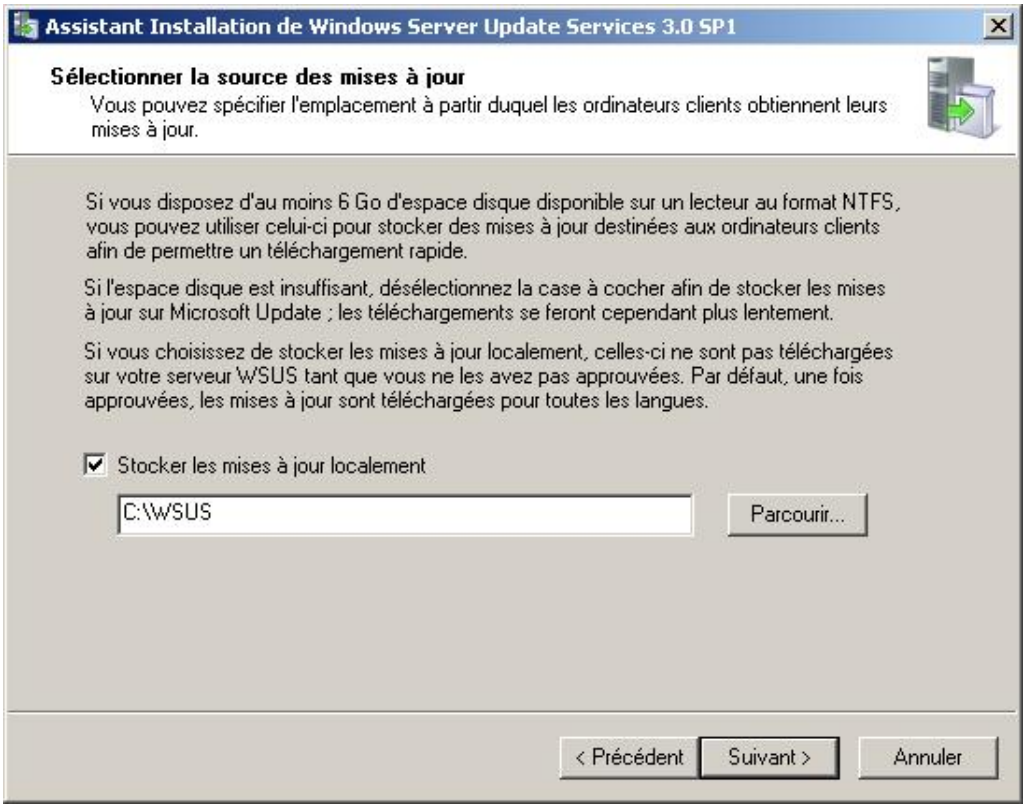
- Fonctionnalités HTTP Communes (incluant Contenu statique)
- Sous Développement d'applications : ASP.NET, Extensions ISAPI
- Sous Sécurité : Authentification Windows
- Sous Outils de Gestion : Compatibilité avec la métabase IIS6

Vous devez également avoir installé : Microsoft Report Viewer 2005, disponible à l'adresse : http://www.microsoft.com/downloads/ details.aspx?displaylang=fr&FamilyID=8a166cac-758d-45c8-b637-dd7726e61367

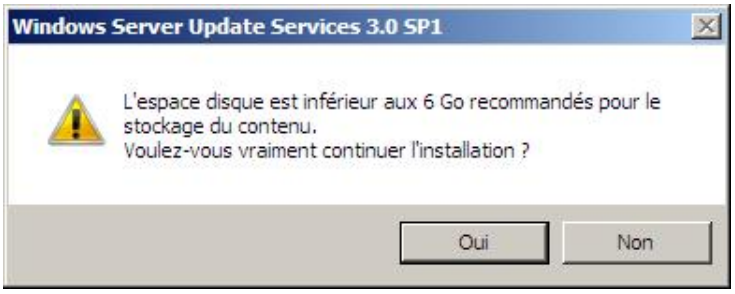
Voici les étapes à suivre pour installer WSUS :

- Lancez l'exécutable d'installation de WSUS.
- À la page de présentation cliquez sur **Suivant**.
- Choisissez **Installation serveur complète avec la Console d'administration** puis cliquez sur **Suivant**.
- Acceptez les termes du contrat puis cliquez sur **Suivant**.
- Spécifiez l'emplacement où WSUS va stocker les mises à jour (ici laissez par défaut) puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Assistant Installation de Windows Server Update Services 3.0 SP1
Sélectionner la source des mises à jour
Vous pouvez spécifier l'emplacement à partir duquel les ordinateurs clients obtiennent leurs mises à jour.
Si vous disposez d'au moins 6 Go d'espace disque disponible sur un lecteur au format NTFS, vous pouvez utiliser celui-ci pour stocker des mises à jour destinées aux ordinateurs clients afin de permettre un téléchargement rapide.
Si l'espace disque est insuffisant, désélectionnez la case à cocher afin de stocker les mises à jour sur Microsoft Update ; les téléchargements se feront cependant plus lentement.
Si vous choisissez de stocker les mises à jour localement, celles-ci ne sont pas téléchargées sur votre serveur WSUS tant que vous ne les avez pas approuvées. Par défaut, une fois approuvées, les mises à jour sont téléchargées pour toutes les langues.
Stocker les mises à jour localement
C:\WSUS
Parcourir...
< Précédent
Suivant >
Annuler

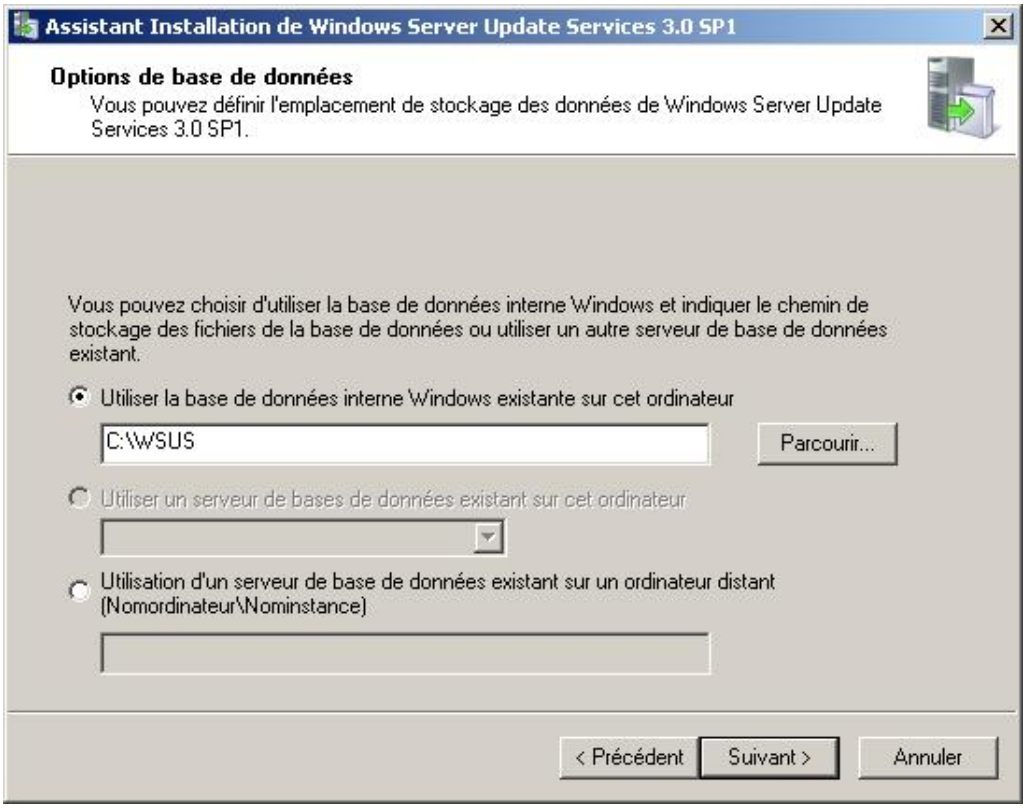
Si la partition sur laquelle vous stockez les mises à jour dispose de moins de 6 Go de libres vous obtenez le message suivant :


Windows Server Update Services 3.0 SP1
L'espace disque est inférieur aux 6 Go recommandés pour le stockage du contenu.
Voulez-vous vraiment continuer l'installation ?
Oui
Non

- Choisissez le serveur qui va héberger la base de données WSUS. Ici choisissez la base de données interne Windows puis cliquez sur **Suivant**.

  Vous avez la possibilité d'utiliser un serveur SQL distant ou même une instance SQL localement installée.

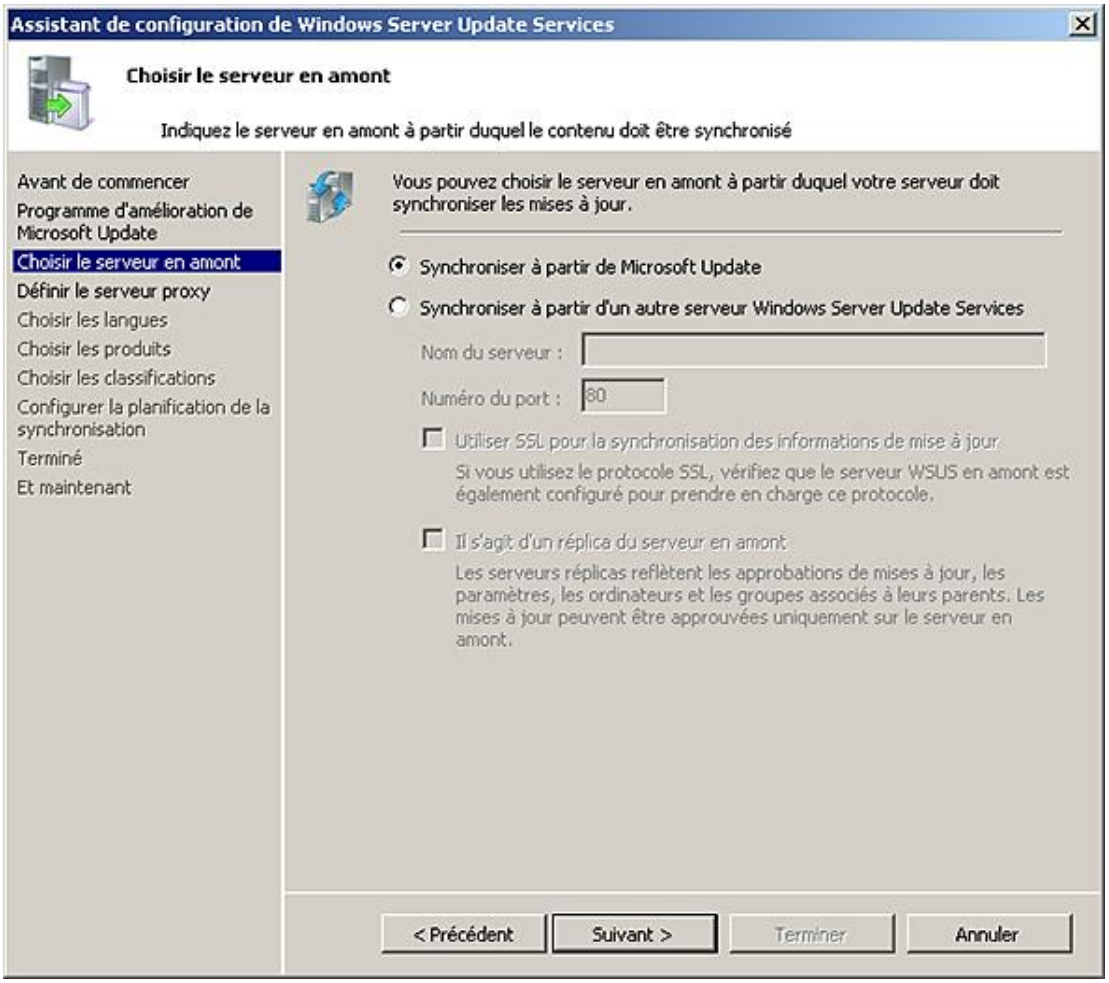
© ENI Editions - All rigths reserved


Assistant Installation de Windows Server Update Services 3.0 SP1
Options de base de données
Vous pouvez définir l'emplacement de stockage des données de Windows Server Update Services 3.0 SP1.
Vous pouvez choisir d'utiliser la base de données interne Windows et indiquer le chemin de stockage des fichiers de la base de données ou utiliser un autre serveur de base de données existant.
Utiliser la base de données interne Windows existante sur cet ordinateur
C:\WSUS
Parcourir...
Utiliser un serveur de bases de données existant sur cet ordinateur
Utilisation d'un serveur de base de données existant sur un ordinateur distant (Nomordinateur\Nominstance)
< Précédent
Suivant >
Annuler

- Validez que la connectivité est opérationnelle puis cliquez sur **Suivant**.
- Choisissez **Créer un site Web Windows Server Update Services 3.0 SP1** puis cliquez sur **Suivant**.
- Validez les informations de configuration puis cliquez sur **Suivant**.
- Une fois l'installation terminée, cliquez sur **Terminer**, la page de configuration va se lancer automatiquement.
- À la page de présentation de la configuration, cliquez sur **Suivant**.
- Laissez la case qui permet de participer au programme d'amélioration cochée puis cliquez sur **Suivant**.
- Laissez la case **Synchroniser à partir de Microsoft Update** cochée puis cliquez sur **Suivant**.

  Sur cette page vous avez la possibilité de spécifier un autre serveur WSUS comme source. Très pratique lorsque vous avez besoin de gérer plusieurs serveurs de mise à jour.

© ENI Editions - All rigths reserved


Assistant de configuration de Windows Server Update Services
Choisir le serveur en amont
Indiquez le serveur en amont à partir duquel le contenu doit être synchronisé
Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Et maintenant
Vous pouvez choisir le serveur en amont à partir duquel votre serveur doit synchroniser les mises à jour.
Synchroniser à partir de Microsoft Update
Synchroniser à partir d'un autre serveur Windows Server Update Services
Nom du serveur :
Numéro du port :
80
Utiliser SSL pour la synchronisation des informations de mise à jour
Si vous utilisez le protocole SSL, vérifiez que le serveur WSUS en amont est également configuré pour prendre en charge ce protocole.
Il s'agit d'un réplica du serveur en amont
Les serveurs réplicas reflètent les approbations de mises à jour, les paramètres, les ordinateurs et les groupes associés à leurs parents. Les mises à jour peuvent être approuvées uniquement sur le serveur en amont.
< Précédent
Suivant >
Terminer
Annuler

- Si vous n'utilisez pas de proxy, n'indiquez rien au niveau de la page proxy puis cliquez sur **Suivant**.

  Autrement, cette page permet si vous utilisez un proxy, de spécifier sa configuration.

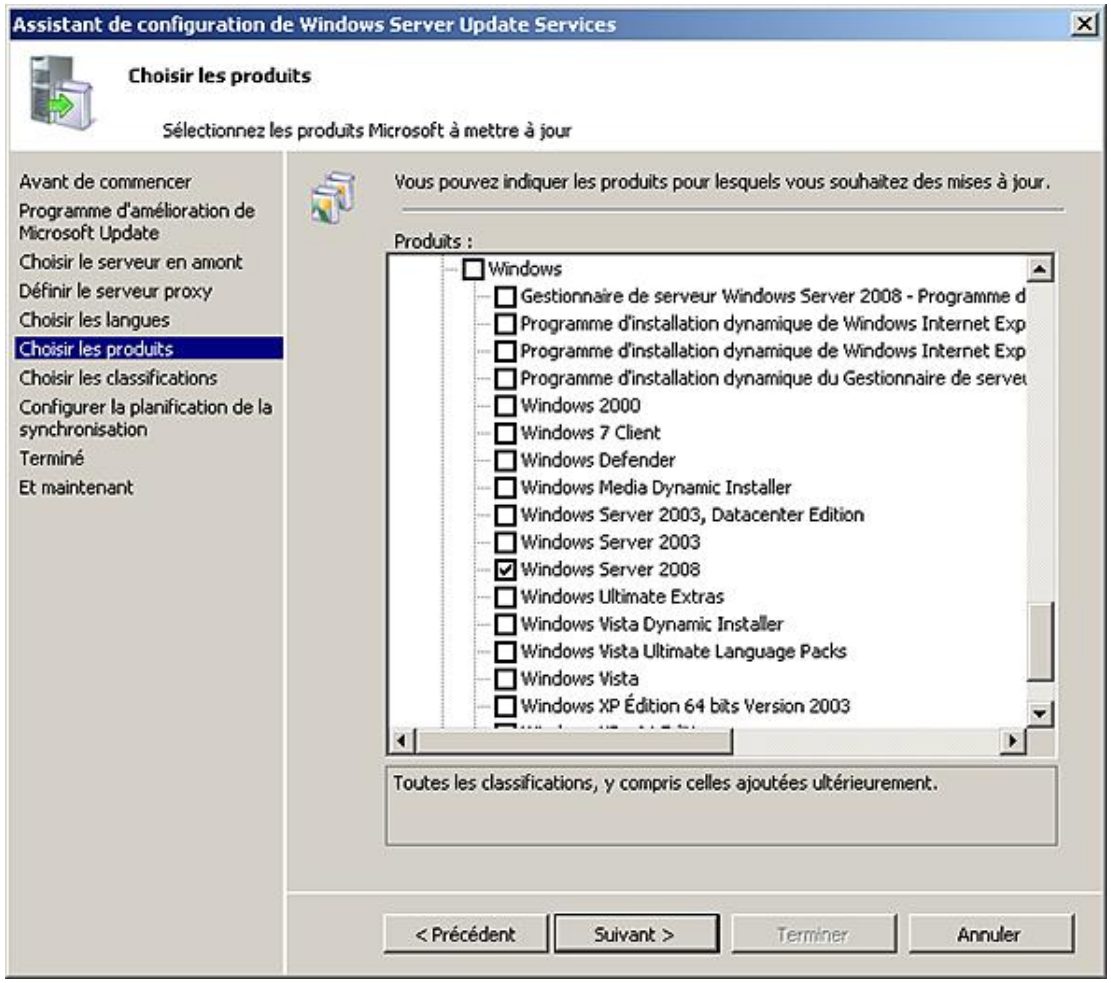
- Cliquez sur **Démarrer la connexion** afin que WSUS récupère les informations disponibles au téléchargement. Une fois la connexion terminée, cliquez sur **Suivant**.

- Sélectionnez les langues utilisées par vos différents systèmes d'exploitation (dans notre exemple français), si ce n'est pas déjà fait automatiquement puis cliquez sur **Suivant**.

Attention à ne pas sélectionner trop de langues sans quoi la taille du répertoire de stockage des mises à jour grandira dangereusement.

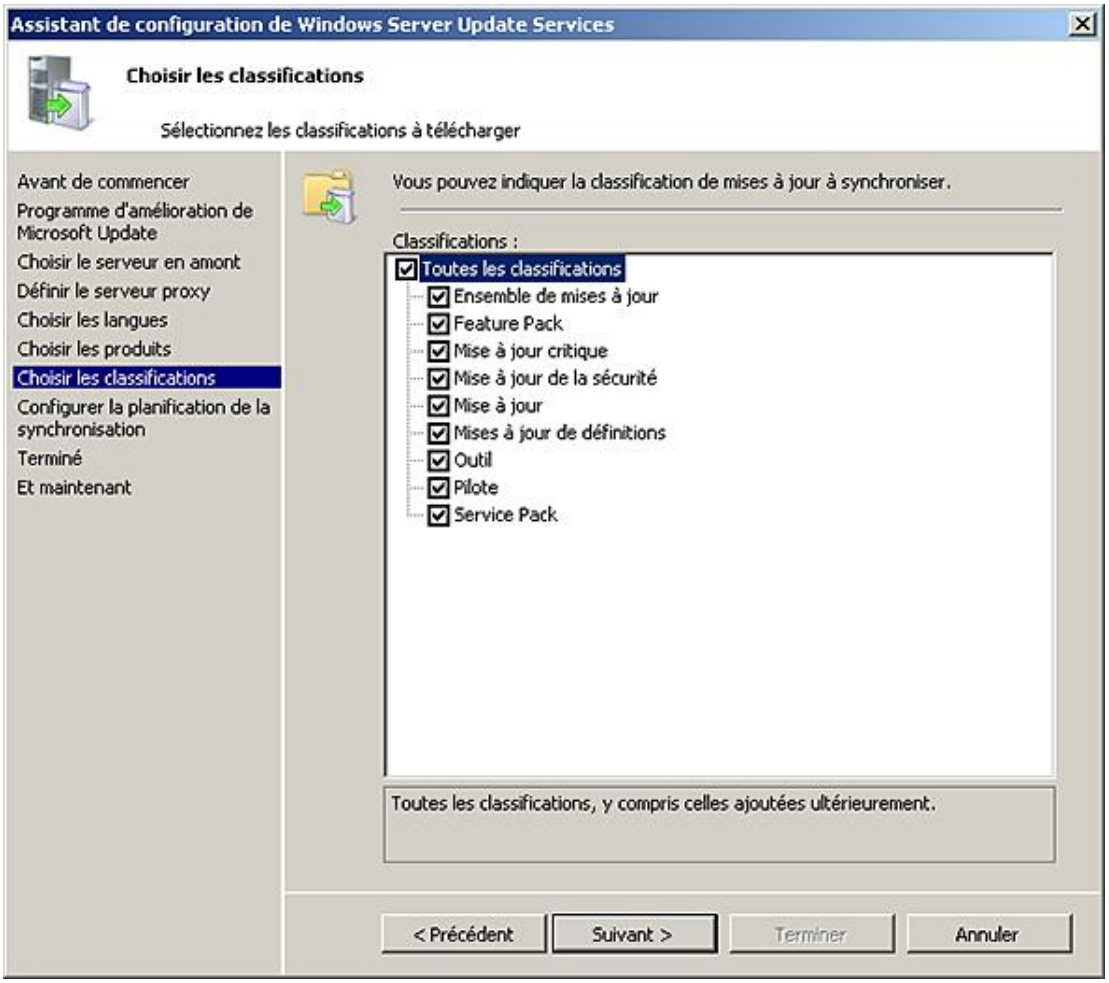
- Dans la liste de sélection des produits, sélectionnez les produits que vous souhaitez mettre à jour (dans notre exemple, nous ne souhaitons mettre à jour que les systèmes d'exploitation **Windows Server 2008**) puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved


Assistant de configuration de Windows Server Update Services
Choisir les produits
Sélectionnez les produits Microsoft à mettre à jour
Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Et maintenant
Vous pouvez indiquer les produits pour lesquels vous souhaitez des mises à jour.
Produits :
Windows
Gestionnaire de serveur Windows Server 2008 - Programme d
Programme d'installation dynamique de Windows Internet Exp
Programme d'installation dynamique de Windows Internet Exp
Programme d'installation dynamique du Gestionnaire de serve
Windows 2000
Windows 7 Client
Windows Defender
Windows Media Dynamic Installer
Windows Server 2003, Datacenter Edition
Windows Server 2003
Windows Server 2008
Windows Ultimate Extras
Windows Vista Dynamic Installer
Windows Vista Ultimate Language Packs
Windows Vista
Windows XP Édition 64 bits Version 2003
Toutes les classifications, y compris celles ajoutées ultérieurement.
< Précédent
Suivant >
Terminer
Annuler

- Les classifications représentent les types de mises à jour que vous souhaitez valider. Cochez la case **Toutes les classifications** puis cliquez sur **Suivant**.

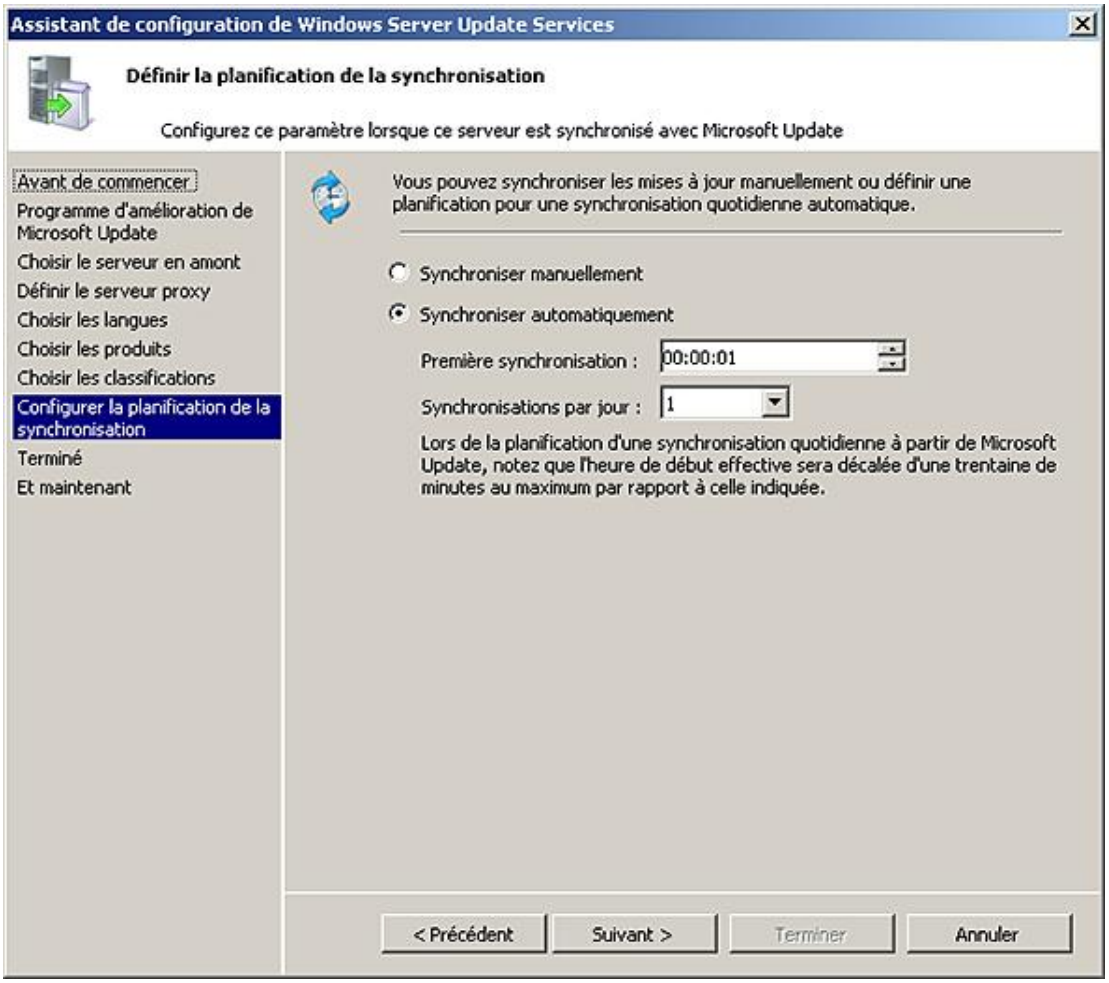
© ENI Editions - All rigths reserved



- Choisissez **Synchroniser automatiquement**, dans la liste déroulante **Première synchronisation**, saisissez **00:00:01**.

- Laissez à 1 synchronisation par jour puis cliquez sur **Suivant**.

© ENI Editions - All rigths reserved

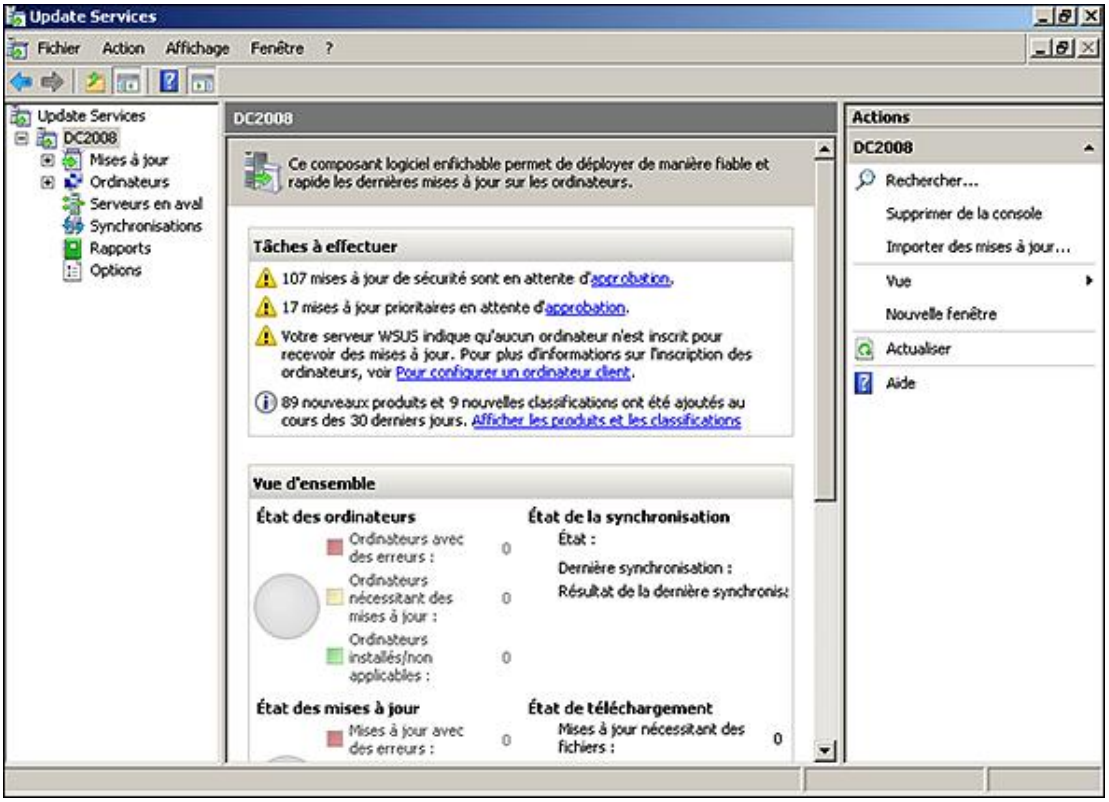

Assistant de configuration de Windows Server Update Services
Définir la planification de la synchronisation
Configurez ce paramètre lorsque ce serveur est synchronisé avec Microsoft Update
Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Et maintenant
Vous pouvez synchroniser les mises à jour manuellement ou définir une planification pour une synchronisation quotidienne automatique.
Synchroniser manuellement
Synchroniser automatiquement
Première synchronisation :
00:00:01
Synchronisations par jour :
1
Lors de la planification d'une synchronisation quotidienne à partir de Microsoft Update, notez que l'heure de début effective sera décalée d'une trentaine de minutes au maximum par rapport à celle indiquée.
< Précédent
Suivant >
Terminer
Annuler

- Une fois la synchronisation finalisée, cliquez sur **Terminer**.

3. Utilisation de WSUS

Une fois l'outil installé, sa console MMC d'administration s'ouvre automatiquement. Vous pouvez y voir rapidement l'état de mise à jour de votre parc ainsi que les mises à jour en attente d'approbation.

© ENI Editions - All rigths reserved


Update Services
Fichier Action Affichage Fenêtre ?
Update Services
DC2008
Mises à jour
Ordinateurs
Serveurs en aval
Synchronisations
Rapports
Options
DC2008
Ce composant logiciel enfichable permet de déployer de manière fiable et rapide les dernières mises à jour sur les ordinateurs.
Tâches à effectuer
107 mises à jour de sécurité sont en attente d'approbation.
17 mises à jour prioritaires en attente d'approbation.
Votre serveur WSUS indique qu'aucun ordinateur n'est inscrit pour recevoir des mises à jour. Pour plus d'informations sur l'inscription des ordinateurs, voir Pour configurer un ordinateur client.
89 nouveaux produits et 9 nouvelles classifications ont été ajoutés au cours des 30 derniers jours. Afficher les produits et les classifications
Vue d'ensemble
État des ordinateurs
Ordinateurs avec des erreurs : 0
Ordinateurs nécessitant des mises à jour : 0
Ordinateurs installés/non applicables : 0
État de la synchronisation
État :
Dernière synchronisation :
Résultat de la dernière synchronis
État des mises à jour
Mises à jour avec des erreurs : 0
État de téléchargement
Mises à jour nécessitant des fichiers : 0
Actions
DC2008
Rechercher...
Supprimer de la console
Importer des mises à jour...
Vue
Nouvelle fenêtre
Actualiser
Aide

Cette console est accessible depuis les **outils d'administration** dans le menu **Démarrer : Microsoft Windows Server Update Services 3.0 SP1**.

Avant tout, il faut que vous configuriez vos clients pour utiliser votre serveur WSUS nouvellement installé.

Si vous disposez d'un domaine Active Directory, créez une nouvelle stratégie de groupe GPO au niveau du domaine ou d'une OU. Si votre PC n'est pas dans un domaine, utilisez la commande `gpedit.msc`.

- Dans l'**éditeur d'objets de stratégie de groupe**, développez **Configuration ordinateur - Modèles d'administration - Composants Windows - Windows Update**.
- Dans le volet de droite, éditez le paramètre **Spécifier l'emplacement intranet du service de Mise à jour Microsoft**.
- Cochez la case **Activé** puis saisissez l'url d'accès à votre serveur WSUS dans les deux champs.

  Exemple : http://dc2008.masociete.local
- Cliquez ensuite sur **Appliquer** puis **OK**.
- Éditez ensuite le paramètre **Configuration du service Mises à jour automatiques**.

  Cochez la case **Activé** puis spécifiez la configuration des mises à jour automatiques (**notifier pour télécharger et installer**, **télécharger et planifier l'installation**, etc.).

  Choisissez ensuite les jours et heures des installations des mises à jour.
- Validez en cliquant sur **Appliquer** puis **OK**.
- Fermez ensuite votre éditeur de stratégie de groupes.

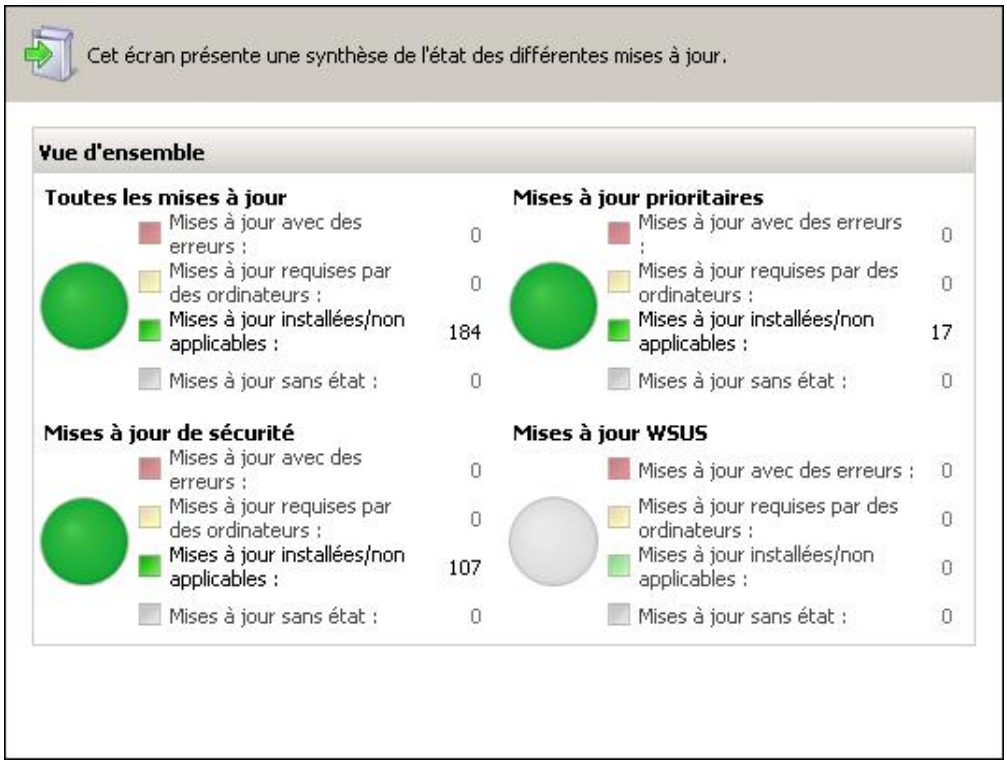
Vous pouvez forcer le rafraîchissement de la stratégie de groupe sur le poste client via la commande `gpupdate`.

Pour forcer la détection par WSUS d'une machine cliente, lancez depuis le poste la commande `wuauclt /detectnow`.

© ENI Editions - All rigths reserved

Depuis la console **Microsoft Windows Server Update Services**, vous pouvez ensuite voir l'état de déploiement des mises à jour.

- Développez l'arborescence et cliquez sur **Mises à jour**.


Cet écran présente une synthèse de l'état des différentes mises à jour.
Vue d'ensemble
Toutes les mises à jour
Mises à jour avec des erreurs : 0
Mises à jour requises par des ordinateurs : 0
Mises à jour installées/non applicables : 184
Mises à jour sans état : 0
Mises à jour prioritaires
Mises à jour avec des erreurs : 0
Mises à jour requises par des ordinateurs : 0
Mises à jour installées/non applicables : 17
Mises à jour sans état : 0
Mises à jour de sécurité
Mises à jour avec des erreurs : 0
Mises à jour requises par des ordinateurs : 0
Mises à jour installées/non applicables : 107
Mises à jour sans état : 0
Mises à jour WSUS
Mises à jour avec des erreurs : 0
Mises à jour requises par des ordinateurs : 0
Mises à jour installées/non applicables : 0
Mises à jour sans état : 0

Des vues préconfigurées sont disponibles. Elles répondent aux besoins de la majorité des administrateurs. Vous pouvez cependant créer des vues personnalisées si vous avez besoin d'informations particulières. Les critères sont nombreux : par produit, par classification, par groupes, etc.

Il vous est également possible d'obtenir des rapports détaillés sur les mises à jour. Il suffit pour cela d'aller dans la rubrique associée et de choisir le rapport à visualiser.

© ENI Editions - All rigths reserved

Cet écran présente les rapports disponibles.
Rapports de mise à jour
Synthèse de l'état des mises à jour
Ce rapport fournit une synthèse de l'état des mises à jour, avec une page par mise à jour.
État détaillé des mises à jour
Ce rapport fournit une synthèse de l'état des mises à jour, avec le statut de mise à jour de tous les ordinateurs pour chaque mise à jour. Chaque page affiche une mise à jour.
Tableau de l'état des mises à jour
Ce rapport fournit une synthèse de l'état des mises à jour sous forme de tableau susceptible d'être exporté dans une feuille de calcul.
Rapports d'ordinateur
Synthèse de l'état des ordinateurs
Ce rapport fournit une synthèse de l'état des ordinateurs, en présentant un ordinateur par page.
État détaillé des ordinateurs
Ce rapport fournit des informations sur l'état de chaque ordinateur avec l'état des différentes mises à jour, en présentant un ordinateur par page.
Tableau de l'état des ordinateurs
Ce rapport fournit une synthèse de l'état des ordinateurs sous forme de tableau susceptible d'être exporté dans une feuille de calcul.
Rapports de synchronisation
Résultats de la synchronisation
Ce rapport fournit les résultats de la dernière synchronisation.

Des rapports préconfigurés sont mis à votre disposition. Vous n'avez pas la possibilité d'en créer de nouveaux. Les modèles préexistants sont générés à la demande de façon à avoir les informations les plus à jour possibles.

La rubrique **Options** vous permet de configurer les options déjà spécifiées à l'installation (langues, classifications, produits, etc.) ainsi que d'autres paramètres :

- **Approbations automatiques** : permet de définir la façon dont sont appliquées les types de mises à jour (sécurité, critiques) pour des ordinateurs définis.
- **Notifications électroniques** : permet d'envoyer des notifications de rapports sur les mises à jour par mail.
- **Assistant de nettoyage du serveur** : permet de nettoyer les anciens ordinateurs, les anciennes mises à jour et les anciens fichiers de mise à jour.
- **Ordinateurs** : permet de spécifier si les groupes d'ordinateurs pour la mise à jour sont gérés depuis WSUS ou via une stratégie de groupe.
- **Personnalisation** : permet dans le cas d'utilisation de serveurs WSUS « enfants » d'avoir un état des ordinateurs qui lui sont associés.
- **Cumul des rapports** : permet dans le cas d'une architecture avec un WSUS frontal d'avoir une centralisation de tous les WSUS « enfants ».

Vous avez vu grâce à ce chapitre des éléments essentiels à la sécurisation de votre parc. En matière de système informatique il ne vaut mieux pas se contenter d'agir après coup. Soyez proactif, et vous gagnerez en rapidité pour remettre votre infrastructure en état de marche en cas de problème majeur.

Pensez votre schéma de sauvegarde en fonction de vos besoins (volume, plage horaire, etc.). Les clichés instantanés

© ENI Editions - All rigths reserved

sont un très bon complément à l'outil de sauvegarde Windows Server Backup. N'hésitez pas également à vous tourner vers des produits tiers comme celui de Microsoft (System Center Data Protection Manager). Ils vous offriront une granularité supplémentaire ainsi que des possibilités étendues de sauvegarde de vos applications (Exchange, SQL, SharePoint, etc.).

Vous prémunir face aux menaces comme les virus, exploitations de failles et autres désagréments est également indispensable. Avoir vos applications toujours à jour permet de corriger les défauts de celles-ci. WSUS est gratuit profitez-en, il vous facilitera grandement la difficile tâche de la gestion des patchs de sécurité Microsoft. Plus besoin de passer individuellement sur chaque PC pour contrôler l'état de mise à jour, ni même pour forcer les mises à jour. Tout est désormais gérable à distance, de façon centralisée et simplifiée.

© ENI Editions - All rigths reserved

L'après Windows Server 2008

Le contenu de la prochaine version de Windows Server est assez bien connu, car Microsoft a présenté des nouvelles fonctionnalités ou évolutions lors de différents évènements tels que l'IT-Forum 2008. Par ailleurs, certains chapitres de cet ouvrage vous ont déjà décrits une partie de ces évolutions prévues.

Les évolutions portent sur 4 axes principaux :

- la virtualisation ;
- l'administration ;
- l'environnement Web ;
- la fiabilité et l'adaptation à tout environnement.

Cette nouvelle version a aussi pour but d'utiliser toutes les nouvelles fonctionnalités du client Windows 7.

Elle prend également en compte les évolutions dans l'administration des services IT, notamment la migration vers des datacenters, l'administration à distance, l'externalisation et le turn-over important des administrateurs n'ayant que peu d'expériences.

D'autres évolutions moins visibles comme le **Core Parking** permettent de réaliser des économies d'énergie (et de chaleur) en adaptant le nombre de processeurs effectivement actifs en fonction de la charge.

Voici quelques informations complémentaires, mais non exhaustives sur chacun de ces points.

1. L'administration

a. PowerShell Version 2.0

La nouvelle version de PowerShell apporte des fonctionnalités très demandées par les passionnés de scripts PowerShell avec notamment l'exécution de scripts à distance sur une ou plusieurs machines. Par ailleurs, il est enfin possible de l'installer sur Windows en version **Core**. Avec l'ajout de **.Net**, on va pouvoir envisager l'installation de nombreux logiciels comme Exchange, par exemple.

La notion d'espace de travail ou d'environnement permet de sécuriser et de bien cloisonner le fonctionnement de chaque script pour une sécurité accrue.

Nombreuses autres possibilités, comme près de 50 commandes supplémentaires pour gérer les services Web, ainsi qu'un outil graphique d'aide au débogage et à la réalisation de script Powershell seront très appréciées.

b. Une poubelle pour les objets Active Directory

L'activation de cette option permet de faciliter la récupération des objets supprimés. Actuellement, il était souvent nécessaire d'acheter des outils supplémentaires pour réaliser ce type d'opération.

c. Le centre Administratif de AD

Il s'agit d'un outil simplifiant l'administration de base des utilisateurs pour les opérations courantes. Cet outil ne remplace pas l'outil habituel de gestion des utilisateurs.

d. L'intégration Hors-ligne au domaine

L'installation des futurs ordinateurs membres peut être réalisée sans que le domaine soit accessible. Ceci va s'avérer très pratique pour les entreprises qui passent par un intégrateur pour l'installation de leurs machines. Un fichier XML de configuration est inclut à l'image.

e. L'administration des serveurs distants

© ENI Editions - All rigths reserved

Avec la Remote Server Manager, on peut gérer les rôles et les fonctionnalités de n'importe quel serveur distant avec n'importe quelle instance de Server Manager.

f. Un analyseur intégré des meilleures pratiques

Fort du succès des outils tels que EXBPA (*Exchange Best Practices*), un outil de validation des informations de configuration de chacun des rôles a été intégré.

2. La virtualisation

La virtualisation et la création de **Virtual Data Centers** permettant de consolider les serveurs et la charge de travail sont des points clés de nombreuses stratégies actuelles. HyperV V2 améliore la prise en charge d'environnements de plus en plus puissants, notamment en prévoyant de gérer jusqu'à 128 processeurs logiques pour la version DataCenter.

a. La virtualisation HyperV V2

Windows 2008 R2 inclut la fonction **Live migration** qui rend la bascule entre deux nœuds presque instantanée. Cette bascule n'est pratiquement pas décelable au niveau des postes clients.

b. La gestion dynamique de la mémoire (Memory Escrow)

Cette gestion dynamique apporte jusqu'à 50 % de mémoire supplémentaire par rapport à Windows 2008 en augmentant ou diminuant la mémoire virtuelle allouée aux machines.

c. La virtualisation basée sur Terminal Server/Enhanced VDI

Avec VDI, les programmes distribués par TS apparaissent directement dans le menu Démarrer sur le poste client des utilisateurs.

La virtualisation du bureau à distance permet aux utilisateurs distants de se connecter à un serveur et d'exécuter des applications ou même des systèmes d'exploitation complets.

Celle-ci supporte Direct X 10.1, Direct 3D, dont les commandes sont envoyées directement sur le client. Le son est supporté dans les deux sens, une vraie communication pourra enfin s'établir !

Cette technologie permet pratiquement d'utiliser plusieurs systèmes différents sur le même OS.

3. L'environnement Web (IIS)

a. L'administration simplifiée

Le déploiement de nouveaux sites Web de manière automatisée ou non par Powershell a été simplifié. L'activation de l'audit (la trace des modifications de configuration), la publication en un clic, la sécurité étendue par URLScan 3.0 sont autant de nouvelles possibilités bien pratiques.

L'utilisation d'un service FTP qui peut enfin être sécurisé nativement fait aussi énormément plaisir.

b. Le support de .Net en mode Core

De nombreuses applications peuvent maintenant être hébergées directement sur un serveur en mode Core, qui sera donc plus rapide et plus sûr.

c. NLB/Cluster

La fonction **Cluster** a été améliorée et prend en compte de nouveaux services dits **Cluster-Aware** : DFS-R, HyperV, TS Session Broker, DHCP,….

Un outil d'analyse (BPA) permet de vérifier la configuration du cluster.

© ENI Editions - All rigths reserved

D'autres fonctions ont été améliorées : un meilleur support des liaisons lentes entre nœuds de cluster mais aussi un maintien optimisé des connexions IP avec un nœud spécifique pour les clusters NLB (Ip Skickiness).

À noter que Powershell remplace maintenant cluster.exe pour la configuration !

4. Les améliorations Windows

Il n'est pas possible de décrire toutes les avancées qui peuvent encore évoluer, sachant que certaines ne sont prévues pour ne fonctionner qu'avec Windows Vista, voire seulement Windows 7.

a. Le cache de sites (Branch Caching)

Ce système consiste à utiliser les stations ou un serveur local pour mettre en cache (un peu comme le font les proxies Internet) les fichiers provenant de serveurs de fichiers (SMB) ou de serveurs Web (http) du site central. Ceci est particulièrement efficace sur les liaisons faibles de type WAN ou VPN.

L'activation se fait par stratégie, en indiquant soit le serveur du site chargé d'héberger le cache, soit l'utilisation de l'ensemble des stations dans un cache **coopératif**. Si un document a déjà été téléchargé par un autre utilisateur, celui-ci sera transmis directement à partir du cache après vérification de la sécurité et de la validité du document. La stratégie peut limiter cette fonctionnalité à certains types de fichiers (.EXE, .DLL, etc.).

b. Un nouveau type d'accès à distance (Direct access feature)

Ce nouveau type d'accès à distance n'a plus besoin de connexion VPN. Concrètement, les connexions sont encapsulées dans HTTP et transmises aux serveurs de l'entreprise.

En fait, la connexion au réseau de l'entreprise se fait avant l'ouverture de session. Si tous les prérequis (Client NAP valide) ont été satisfaits, alors les requêtes à destination des serveurs de l'entreprise sont détectées et acheminées par un tuyau en IP V6 jusqu'au réseau de l'entreprise.

Contrairement à une connexion VPN classique, seul le trafic utile est envoyé dans le tunnel.

c. L'amélioration de la sécurité

Tous les lecteurs amovibles sont mieux protégés par l'utilisation de BitLocker.

L'utilisation des serveurs DNS est sécurisée par l'utilisation de certificats. Un serveur DNS peut vérifier l'authenticité d'un enregistrement reçu d'une zone signée. Les clients peuvent établir une relation sécurisée avec le serveur.

d. Le déploiement physique et virtuel

Devenu un standard de fait pour démarrer rapidement une machine virtuelle, le boot à partir d'un fichier VHD permettra d'utiliser une image identique pour installer les machines physiques et virtuelles.

Ceci n'était qu'une présentation très succincte d'une partie des éléments connus sur la nouvelle version mais cela vous donne un avant goût de ce que vous réserve l'avenir.

© ENI Editions - All rigths reserved

Le calendrier attendu

Jusqu'à présent, les beta-testeurs disposaient d'une version M3 dont le noyau était commun pour la future version du client Windows 7 et du serveur. La prochaine version devrait s'appeler **Windows 2008 R2 Server**. Néanmoins, son numéro interne sera en 7000.

Une première version Beta de Windows 2008 R2 est librement téléchargeable dès à présent en version anglaise sur le site de Microsoft. Attention, cette prochaine version n'est prévue **que** pour les systèmes 64 bits. En revanche, les autres pré-requis sont les mêmes que pour Windows 2008.

Windows 7 client et Windows 2008 R2 devraient sortir relativement simultanément, probablement début Janvier 2010. Mais, des surprises sont toujours possibles !

© ENI Editions - All rigths reserved